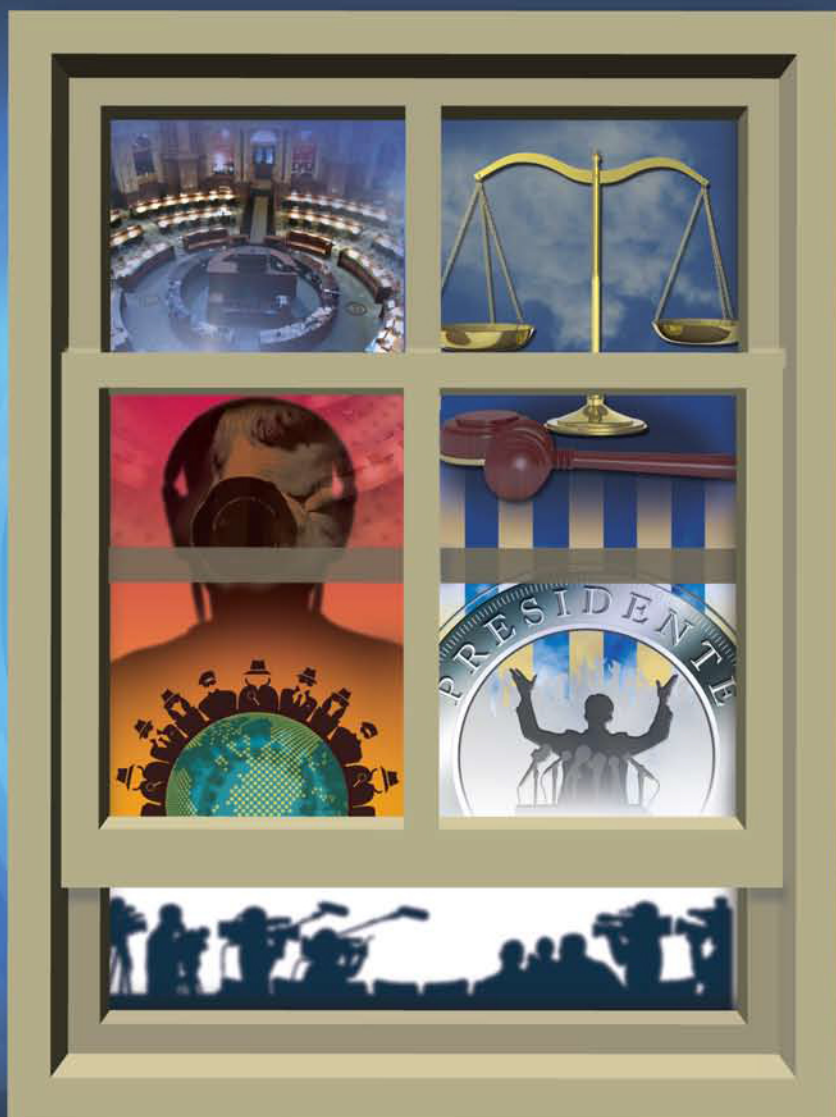


# GESTIÓN DE INTELIGENCIA EN LAS AMÉRICAS



Russell G. Swenson y Carolina Sancho Hirane  
Editores

NATIONAL INTELLIGENCE UNIVERSITY

# Gestión de Inteligencia en las Américas

Coordinadores

Russell G. Swenson

y

Carolina Sancho Hirane



Universidad Nacional de Inteligencia  
Washington, DC  
Julio 2015



Esta antología, *Gestión de Inteligencia en las Américas*, reúne las perspectivas de autores de países a través de las Américas. Esbozan y evalúan el status y oportunidades para legislación y otras opciones de supervisión y control de inteligencia, y abarcan varios argumentos por la preservación de los aspectos más beneficiosos de la autonomía de la función.

La meta de la NI Press es dar luz a libros de calidad, de manera oportuna, sobre temas de interés a las comunidades de inteligencia de los Estados Unidos y de otras de la región. Los documentos originando de la NI Press se someten a revisión pre-publicación por oficiales mayores del gobierno de los Estados Unidos, tanto como por expertos externos.

Este libro ha sido aprobado para una difusión ilimitada por la Oficina de Revisión de Seguridad del Departamento de Defensa de los Estados Unidos. Declaraciones sobre hechos, de opinión o de análisis expresadas por los autores son solamente de ellos, y no representan las políticas oficiales de sus respectivas oficinas, ministerios o gobiernos. Los autores disfrutan de libertad de expresión completa, a la medida que no se presenta información clasificada, no se perjudica la seguridad operativa, y no se representan erróneamente las políticas oficiales de los Estados Unidos. Esta libertad académica habilita a los autores ofrecer nuevas y a veces contenciosas perspectivas con el propósito de avanzar el debate sobre temas claves. Esta publicación se produce bajo autoridad de Título 17, Código de Ley de Estados Unidos, secciones 101 y 105. Está en el dominio público, y no se puede pedir ni dotar fuero de propiedad intelectual (copyright) en su totalidad.

Cómo obtener ejemplares del libro: Todos pueden bajar una copia electrónica del libro gratis desde la página de la prensa en <http://www.NI-U.edu>. Empleados del gobierno estadounidense pueden pedir un ejemplar gratis mediante comunicación con [press@NI-U.edu](mailto:press@NI-U.edu). El público en general puede buscar y comprar ejemplares de la Oficina Gubernamental de Prensa (GPO) en <http://bookstore.gpo.gov>.

Editor, NI Press  
Office of Research  
National Intelligence University  
Defense Intelligence Agency  
Joint Base Anacostia Bolling  
Washington, DC 20340-5100

ISBN  
Biblioteca del Congreso número de control

978-1-932946-44-4  
2012948537

## Contenidos

Tablas .....	vii
Ilustraciones .....	viii
Prefacio de los Coordinadores .....	ix
Reconocimientos .....	xi
<b>Introducción</b>	
Gestión de la Inteligencia del Estado .....	xiii
— <i>Russell G. Swenson</i>	
<b>Sección I—Fiscalización de Inteligencia en el Contexto</b>	
<b>Democrático: Dimensiones Éticas y Legales .....</b>	<b>1</b>
Revisão da Primeira Secção.....	3
— <i>Marco Cepik</i>	
Leyes de Inteligencia en el Perú y Latinoamérica: Evolución Histórica, Jurídica e Institucional .....	5
— <i>Andrés Gómez de la Torre Rotta con Arturo Medrano Carmona</i>	
Leyes de Inteligencia de Norteamérica, América Central y Sudamérica (Tabla).....	75
— <i>Liza Zúñiga Collado</i>	
Guardando os Guardiães: O Controle dos Serviços Secretos no Regime Democrático .....	89
— <i>Joanisval Brito Gonçalves</i>	
Estado de Supervisión y Control Democrático de los Servicios de Inteligencia (Tabla) .....	117
— <i>Russell G. Swenson y Carolina Sancho Hirane</i>	
Ética e Inteligencia: Revisión de la Experiencia Europea y Norteamericana y su Aplicación en América Latina .....	121
— <i>Carlos Maldonado Prieto</i>	

## Contenidos (a continuación)

Derechos Humanos y Ética de la Inteligencia: Análisis de Casos Cinematográficos .....	143
— <i>Moira Nakousi Salas y Daniel Soto Muñoz</i>	
Inteligencia, Medios de Comunicación, y Discurso Político.....	167
— <i>Manuel I. Balcázar Villareal</i>	
<b>Sección II—Gestión de Inteligencia en la Rama Ejecutiva de los Gobiernos .....</b>	<b>171</b>
Procesos de Toma de Decisión Presidencial en Inteligencia—una Cuestión Pendiente .....	173
— <i>Guillermo Holzmann</i>	
Relación entre Consumidores y Productores de Inteligencia en el Nivel Ejecutivo: Un Desafío Permanente .....	185
— <i>Manuel I. Balcázar Villareal</i>	
Entre el Temor y la Necesidad—un Ensayo de Interpretación Histórica .....	189
— <i>Jorge Jouroff</i>	
La Inteligencia Estratégica y sus Requisitos para la Seguridad en América del Sur .....	201
— <i>Mariano Bartolomé</i>	
Gestión de Inteligencia Económica Gubernamental: Una propuesta para examinar en el Área Andina .....	221
— <i>Álvaro José Venegas González</i>	
Gestión de Recursos para la Inteligencia .....	249
— <i>Dan Elkins</i>	
Cooperación en Inteligencia en el Marco de la Unión de Naciones Suramericanas (UNASUR): Posibilidades y Limitaciones .....	269
— <i>Carolina Sancho Hirane</i>	
<b>Sección III—Gestión de la Privacidad vs. Seguridad y Comunidades de Inteligencia .....</b>	<b>295</b>

## Gestión de Inteligencia en las Américas

### Contenidos (a continuación)

Gestión de la Privacidad vs. Seguridad y Comunidades de Inteligencia .....	297
— <i>José Manuel Ugarte</i>	
Comentarios sobre los Ensayos en la Sección Tres .....	313
— <i>Thomas C. Bruneau</i>	
Os desafios Institucionais no Processo de Integração do Sistema de Inteligência de Segurança Pública Brasileiro .....	317
— <i>Priscila Carlos Brandão</i>	
Inteligencia en el Ámbito Penitenciario: Condiciones para su Relación con la Seguridad Pública .....	343
— <i>Liza Zúñiga Collado</i>	
Autonomía de Inteligencia, Rendición de Cuentas y Seguridad Pública: Fundamentos para su Fiscalización .....	361
— <i>Russell G. Swenson y Zulia Yanzadig Orozco Reynoso</i>	
<b>Sección IV—Gestión de Integración—un Reto para los Servicios de Inteligencia .....</b>	<b>379</b>
Comentario: Educación e Integración en Inteligencia: Una Relación Simbiótica .....	381
— <i>Anne Daugherty Miles</i>	
La Formación del Profesional de la Inteligencia Estratégica: Realizando Expectativas Nacionales .....	385
— <i>José Gabriel Paz</i>	
Manejo y Gestión de la Información de Inteligencia para la Seguridad Multilateral del Ciberespacio-Enfoques de los Estados Unidos y Brasil .....	425
— <i>Robin Rogers</i>	
Captar el Capital Intelectual del Sector de Seguridad: Transformar la Conciencia del Entorno del Asesor en un Entendimiento Socio-Político dentro de un Ambiente de Poder Inteligente (“Smart Power”) .....	453
— <i>William S. Brei, Nathalie J. Frensley and Killaurin O. Roberts</i>	

**Contenidos (a continuación)**

Conclusiones .....	489
— <i>Carolina Sancho Hirane</i>	
Notas de Fuentes Citadas .....	497
Índice .....	585

### Contenidos (a continuación)

#### Tablas

1. Evolución de Legislación en Materia de Inteligencia, 1999-2005 .....	20
2. Comparación de Legislación de Inteligencia Vigente y Derogada en Perú .....	27
3. Leyes de Inteligencia de Norteamérica, América Central y Sudamérica .....	76
4. Estado de Supervisión y Control Democrático .....	117
5. Tipología sobre Formas de Gobierno y Agencias de Inteligencia .....	145
6. Referencias a los Derechos Humanos en las Leyes de Inteligencia Latinoamericanas .....	147
7. Fuentes de Controversias entre la Actividad de Inteligencia y Protección de los Derechos Humanos Ejemplificadas en Determinadas Películas .....	152
8. Ideas que Alimentan las Identidades Únicas .....	159
9. Dos Componentes de Contrainteligencia .....	239
10. Pautas para Acción Colaborativa por un Equipo de Inteligencia Económica Estratégica .....	242
11. Planilla de Resumen de Recursos de Inteligencia .....	262
12. Características Diferenciadoras de los Servicios de Inteligencia Militar, Información Policial e Inteligencia Estratégica .....	274
13. Miembros de la Comunidad o Sistema de Inteligencia en cada país de UNASUR .....	282
14. Posibilidades de Cooperación en Inteligencia en UNASUR .....	286
15. Esquema de Sugestões paro o melhoramento da Inteligência Nacional .....	339
16. Parámetros Académicos de las Instituciones de Estudios en Inteligencia Estratégica .....	411
17. Hoja de Evaluación Curricular (ejemplo) .....	412
18. Hoja de Evaluación del Desempeño Laboral (ejemplo) .....	413
19. Instrucciones de Entrevistar .....	416
20. Hoja de Evaluación de Conocimientos (ejemplo) .....	420
21. Hoja de Resumen de Evaluación Individual (ejemplo) .....	422



## Contenidos (a continuación)

### Ilustraciones

1. Autonomía de la Inteligencia vs. Supervisión y Control .....	xx
2. Balanceo de Esferas de Información para Decisiones en Seguridad Nacional .....	xxiii
3. Tres Perspectivas sobre Inteligencia y Seguridad Ciudadana .....	xxxi
4. Modelos de Integración de Inteligencia .....	xl
5. Principales Justificaciones para las Conductas Inhumanas .....	162
6. Uff. Que riesgosa tarea la de hoy. Esta información bastará para mañana. ....	234
7. Urrg...¿Estás diciendo la verdad, toda la verdad y nada más que la verdad?! .....	237
8. ¡Jefe. Creo que esta vez habrá novedades! .....	240
9. Equipo de Marina Mexicana .....	372
10. Miembros de la Unidad Especial Operativo de Policía “Zorros” ....	373
11. Equipo Policía Federal Mexicano .....	376
12. Esquema del Proceso Evaluación Académica de la Institución .....	405
13. Centros de Ciberseguridad Federal de los Estados Unidos .....	437
14. Instituciones Brasileñas de Ciberseguridad Gubernamental .....	438
15. El Ambiente Operacional Complejo de la Misión de Asesoramiento .....	457
16. Reducir el Espacio entre la Conciencia del Entorno y el Entendimiento en un Problema Hipotético de Reforma del Sector de Seguridad .....	467

### PREFACIO DE LOS COORDINADORES

En cualquier país, la primera línea de protección del pueblo y del sistema de gobierno frente a amenazas las proveen, por definición, las instituciones de inteligencia del Estado. Destacamos de nuestro interés la inteligencia estratégica; es decir, la función que tiene como finalidad la identificación de amenazas, riesgos y oportunidades nacionales, respecto del campo de seguridad del Estado y la seguridad pública o ciudadana.

Desde la década de los 80 en las Américas, se ha trasladado notablemente la responsabilidad para la gestión de una buena parte de la inteligencia del Estado desde las manos militares y policiales hacia una sistema o incipiente comunidad de inteligencia que cuenta con una variedad de entidades de la rama ejecutiva, compuesta por civiles mayoritariamente. Como consecuencia, una adecuada gestión de la función de inteligencia, oportuna y confiable, ahora se extiende mas allá de quienes tradicionalmente han desarrollado esta función -o buscan hacerlo-, observándose un aumento de entidades civiles especializadas que realizan inteligencia, tanto en temas específicos como en la integración de todas aquellos asuntos que pudieran afectar tanto los intereses nacionales como la seguridad del país. Para avanzar en lo señalado falta entonces reflexionar sobre el rol de la ética profesional, leyes públicas de inteligencia, y supervisión jurídica encargada de efectuar un control adecuado sobre la actividad de inteligencia en este ambiente.

Es el propósito del libro atender los desafíos de los contextos actual y futuro de esta función gubernamental. Este propósito nos motiva a identificar, señalar e investigar las huellas del tránsito de responsabilidad de la función, y marcar las buenas prácticas en gestión de inteligencia, siempre tomando en cuenta el ámbito político, social, tecnológico e económico donde funciona esta disciplina cognitiva y muchas veces operativa.

El presente libro cuenta con las observaciones y hallazgos de dos trabajos anteriores de naturaleza académica-aplicada sobre el tema de inteligencia del Estado en el hemisferio. El primero, *Profesionalismo de Inteligencia en las Américas* (2003 y 2004),<sup>1</sup> que aborda el desarrollo del profesionalismo durante la transición democrática en la región, y su estado a inicios del tercer milenio. El siguiente libro, de título *Democratización de la Función de Inteligencia: El Nexo de la Cultura Nacional y la Inteligencia Estratégica* (2009),<sup>2</sup>

## Russell G. Swenson y Carolina Sancho Hirane

se orienta al concepto de cultura nacional de inteligencia como producto y condicionante de las interacciones de la clase política con las instituciones de inteligencia en muchos de los países. Este tercer libro, *La Gestión de Inteligencia en las Américas*, del mismo modo adopta una perspectiva temática para identificar algunas tendencias regionales o sub-regionales que pueden adoptarse para una gestión eficaz de inteligencia del Estado. Asimismo en este libro describimos estas tendencias que generan desafíos a la función de inteligencia, como también investigamos buenas prácticas realizadas que pueden exportarse, junto con señalar algunos temas y tareas pendientes que es necesario abordar.

El libro aprovecha de autores con amplia trayectoria profesional y con experiencia en puestos educativos y/o gubernamentales. Los ensayos en su conjunto presentan un retrato descriptivo y normativo de la función de inteligencia, y aspiramos con este trabajo llamar atención con el objetivo de entender y mejorar la gestión de inteligencia a través de toda la región.

### RECONOCIMIENTOS

La relación profesional de los editores con sus autores suele ser beneficioso para ambos lados, y este ideal colaborativo también caracteriza bien el desarrollo del presente proyecto. Cada autor del libro ha señalado aspectos nuevos de los temas respectivos, superando sus trabajos anteriores para destacar las mejores prácticas, unas ya vigentes y otras para alcanzar, en el desempeño de la gestión de inteligencia a toda escala de aplicación. Los editores, no sólo aprecian la perseverancia y paciencia de los autores, sino además reconocen el apoyo y el consejo de varios críticos (los comentarios de algunos de ellos se encuentran en el libro). Se reconocen Cathryn Thurston, vicepresidenta de Investigaciones Académicas de la NIU, por su apoyo de largo plazo del proyecto, junto con Trina Walsh, Julia Famularo, Katherine Culclasure y George Clifford, de esta oficina; Larry Hiponia, Director, y Steven Carey, del Centro de Enlaces Internacionales, por sus gentilezas varias; Adrienne Young-Battle, Denise Hodges y Donna Wilson, por sus destrezas de diseño gráfico y preparación de manuscritos para la prensa; también a Andrés González Vargas, profesor en la Universidad Jorge Tadeo Lozano, Bogotá, por sus aportes gráficos reproducidos en el ensayo de Álvaro Venegas González. Y finalmente, merecen mención el apoyo editorial y de traducción de William Spracher de la NIU, Liliana Rodríguez de Argentina, Álvaro Venegas de Colombia, y Lydia Marques de la Universidad de Texas. Como de siempre, cualquier error de comisión u omisión es responsabilidad de los editores mismos.



## Gestión de Inteligencia en las Américas

### Gestión de la Inteligencia del Estado

Russell G. Swenson

*Acuérdate, querida, acuérdate. Todos somos espías de niños; esa era la única forma de darle sentido al mundo.*

—Amanda Cross, *An Imperfect Spy*, p. 224.

Los ensayos presentes en este libro examinan el contexto democrático de la gestión de inteligencia en las Américas, donde crecientemente, el control judicial y legislativo complementa con un compromiso ético y profesional a la práctica de la función. Hemos llegado a depender de la inteligencia para la seguridad pública, planificación civil y militar, e incluso nuestro bienestar económico. Un director civil de inteligencia de México esboza esta variedad de intereses y responsabilidades de inteligencia:

Las amenazas (peligros ya presentes) y riesgos (peligros potenciales) no sólo provienen de los llamados temas duros de la seguridad nacional o de las amenazas del exterior, sino también del entorno económico, social y político, e incluso de factores como el medio ambiente. Fenómenos como las tendencias demográficas, las corrientes migratorias, la cohesión y las desigualdades sociales, la economía informal, el rezago respecto de la sociedad del conocimiento y el calentamiento global, son también parte de esta agenda de seguridad nacional.<sup>3</sup>

Tenemos un interés en entender cómo la inteligencia puede comprometer a los líderes civiles de un país así como simplificar la implementación de políticas inteligentes en seguridad pública diplomáticas, militares y económicas. El mismo funcionario de inteligencia mexicano también señala la previsión inequívoca que la inteligencia puede traer a la administración pública relacionada con los asuntos de seguridad nacional:

Esta metodología también le otorga a la agenda nacional un carácter preventivo: desactivar los riesgos provenientes de esos ámbitos, mediante un adecuado sistema de indicadores que permita, en primer lugar, identificar y dimensionar

el daño potencial a los componentes constitutivos de la seguridad nacional (Estado, territorio, población, orden Constitucional, instituciones democráticas, etc.) y, en segundo lugar, alertar a las dependencias del gobierno federal con información adecuada, en tiempo y forma, para actuar con oportunidad. De esta manera, la seguridad nacional se convierte en una política transversal.<sup>4</sup>

La naturaleza de una seguridad nacional que involucra a todo el gobierno, promovida y prolongada por la inteligencia, implica la existencia de una amplia gama de aplicaciones estatales de esta tradicional función del gobierno, a través de numerosos ministerios ejecutivos o departamentos. A nivel nacional, se habla de la inteligencia estratégica, la cual “busca, principalmente, guiar la formulación y la ejecución de medidas de seguridad nacional, en tiempos de paz, y la conducta de operaciones militares, en tiempos de guerra”.<sup>5</sup>

Pero más allá de la inteligencia estratégica del Estado, destinada a las más altas autoridades, ahora tenemos en la región otro tipo de inteligencia que responde a las necesidades ministeriales o departamentales, y al mismo tiempo maneja problemas estratégicos. Como un ejemplo, podemos señalar al Centro de Gestión Operacional del Sistema para la Protección de la Amazonía (CENSIPAM),<sup>6</sup> que como un miembro permanente del Sistema Brasileño de Inteligencia (SISBIN), produce inteligencia para todos sus integrantes. Los riesgos y amenazas en la región Amazónica son a menudo transnacionales y presentan retos a más de un ministerio brasileño, por lo tanto, por una definición comúnmente empleada, estos son problemas del ámbito estratégico.<sup>7</sup> Como otro ejemplo, tenemos disponible una descripción y análisis singular sobre la toma de decisiones dentro de la “Célula de Amenazas Financieras” de las Fuerzas Aliadas en Irak.<sup>8</sup> Esta célula fue la anfitriona de personal de varias organizaciones del gabinete de EE.UU., incluyendo las Fuerzas Armadas y el Departamento del Tesoro. Analistas en esta unidad regularmente tomaron decisiones de consecuencia estratégica como resultado de la orientación que proveyeron a las fuerzas operacionales, y por su contribución directa al desarrollo de una campaña estratégica. Estos ejemplos muestran cómo la función de inteligencia aún opera en ambientes lejanos de la influencia geográfica de la capital nacional, siendo indispensable para un análisis efectivo en contextos donde la información exclusiva contribuye a la implementación de políticas públicas frente a los retos de seguridad.

## Gestión de Inteligencia en las Américas

Hoy en día, el aparato de inteligencia Estatal, incluso en las sociedades más globalizadas, se orienta cada vez más hacia el ambiente doméstico. El ambiente doméstico o interno de un país expone tendencias sociales, psicológicas y económicas que, reconocidas o no como tales, influyen y reflejan condiciones de seguridad en el resto del mundo.

Los retos de seguridad que son de índole local e internacional, incluyen delitos cibernéticos, actos violentos de terrorismo, tráfico de drogas, de armas, y de seres humanos, junto con contrabando, lavado de dinero, y piratería. Una herramienta útil en la vigilancia de quienes pueden generar amenazas a la seguridad de los ciudadanos, y adecuada para generar la información necesaria para evitar su concreción es la inteligencia del Estado. Países como los Estados Unidos y la China, con preocupaciones políticas globales, y el hogar de muchas empresas multinacionales, dedican recursos en una escala asombrosa para mirar hacia el exterior y obtener conocimiento e influencia. Pero en buena medida a través del mundo, el gobierno o la función central de inteligencia se orienta al ambiente interno. Esto se puede confirmar observando los diagramas organizacionales de servicios de inteligencia de diversos países del mundo, quienes dan prioridad administrativa al orden interno.<sup>9</sup>

Otro fenómeno clave que acompaña a esta orientación interna y que hace necesaria la gestión cuidadosa de la función de inteligencia es el énfasis respecto a los derechos de los ciudadanos establecidos y garantizado en las leyes de cada país. ¿Hay realmente una reorientación de doctrina de los servicios de inteligencia, en la medida que se han consolidado las instituciones democráticas en muchos de los países? ¿Es suficiente el control dentro del servicio o del ejecutivo, junto al control externo, para que desde el gobierno no se use la inteligencia contra el ciudadano que incomoda a la autoridad política?

Los encargados de realizar la función de inteligencia, la cual por definición incluye asesorar a los funcionarios electos y a los más altos niveles encargados de la gestión pública, sobrellevan la responsabilidad de cultivar y lograr un entendimiento profundo en asuntos de corto y mediano plazo y de las oportunidades que le acompañan para una acción ejecutiva apropiada. En el presente libro, los autores identifican algunos de estos asuntos que están cambiando constantemente, pero el objetivo del libro no es tratar de catalogarlos ni resolverlos. En cambio, ofrecemos una exploración de los conceptos, los métodos, y la organización de inteligencia con el fin de entenderla como



un fenómeno socio-político y económico sujeta a la gestión en cada Estado-Nación de la región.

Se plantea que una gestión de inteligencia eficaz se orientará hacia el intercambio de información entre los servicios de inteligencia del Estado a nivel nacional como también con sus homólogos internacionales, de acuerdo al apoyo político que brinden las autoridades involucradas en su realización, con el fin de reducir o evitar los actos más peligrosos de las redes criminales transnacionales.

Alcanzar este objetivo dependerá no sólo del profesionalismo de los burócratas del gobierno, sino también en la habilidad de la clase política de aplicar opciones adecuadas a la naturaleza de la función y oportunas con relación al momento en que son requeridas para resolver tensiones claves en el entorno del manejo de la inteligencia.

### Los cuatro niveles de la gestión de inteligencia

Las cuatro secciones del libro abordan puntos de vista distintos sobre la gestión de la inteligencia que son fácilmente distinguibles por su escala de responsabilidad. La primera sección estudia el estatus de pesos y contrapesos incorporados desde el poder Legislativo y poder Judicial, junto al Ejecutivo, para aplicar la supervisión y control de inteligencia en nombre de los ciudadanos del país. En una menor escala institucional, la segunda sección se enfoca en las opciones de gestión desde el poder Ejecutivo. La tercera sección aborda las opciones enfrentadas por el juego de los servicios de inteligencia, o la comunidad de organismos de inteligencia, que debe gestionar la tensión entre la privacidad y la seguridad cuando las capacidades de inteligencia son aplicadas al ambiente interno en países de la región. Finalmente, los servicios de inteligencia, como instrumento de gestión para educar e integrar entidades varias del gobierno, se colocan bajo el microscopio en la última sección.

#### 1. Control y fiscalización de inteligencia en un contexto democrático: pesos y contrapesos de los poderes legislativo, judicial y ejecutivo

*Conceptos clave: Autonomía de inteligencia, leyes nacionales de inteligencia, reglas judiciales, responsabilidad hacia los ciudadanos*

## Gestión de Inteligencia en las Américas

Cualquier régimen que ejerce poder concentrado, considerado o no autoritario, podría utilizar a sus servicios de inteligencia ya sea civil o militar como “policía política”. Ejemplos connotados aparecen en todos los confines del hemisferio, tales como el del Presidente Richard Nixon en su intento de utilizar a la Agencia Central de Inteligencia para encubrir la implicación de su administración en la entrada forzada a Watergate<sup>10</sup> y el uso de chantajes por parte de los jefes del servicio de inteligencia del Presidente Alberto Fujimori del Perú para influenciar a funcionarios públicos.<sup>11</sup>

Con la transición de casi todos los países del hemisferio hacia la condición de contar con regímenes democráticos cada vez más sólidos en las últimas décadas, podemos comenzar a evaluar la gestión democrática de varios aspectos de la inteligencia nacional en nuestra región de interés. Unas investigaciones discuten y comparan el estado de la gestión de la función en Argentina, Brasil, Perú y España.<sup>12</sup>

Matei y Bruneau comentan que la renuencia por parte de los formuladores de políticas (presidentes y líderes políticos de alto nivel) en involucrarse con los asuntos de reforma de la inteligencia los conduce a soluciones incompletas y apresuradas respecto a una mejora de la eficacia de la inteligencia y la posibilidad de asegurar la rendición de cuentas. Su renuencia para abordar la gestión integral de inteligencia se debe a varios factores, entre ellos una carencia de interés público y de las élites políticas en debatir decisiones administrativas y las dudas que genera ser asociados con agencias con cargas negativas, históricamente ligadas a la violación de los derechos humanos. Este distanciamiento permite al personal de inteligencia, nuevamente o durante años, una mayor libertad para presionar por la liberación de acciones y prerrogativas que disfrutaban en anteriores acuerdos burocráticos autoritarios o de ideología liberal (*laissez-faire*). Además, los líderes políticos pueden emplear las capacidades de inteligencia militar no está cuya actividad no está específicamente abordada por leyes o regulaciones.<sup>13</sup> Los autores señalan que los incentivos para una eficaz reforma a la gestión de inteligencia pueden provenir de múltiples direcciones: como resultado de una exposición internacional que se obtiene con la participación en operaciones de paz (el liderazgo de Brasil en operaciones de paz en Haití); una apreciación clara de amenazas serias (Brasil-crimen organizado violento); o una crisis debido a la escasez de inteligencia (Argentina-ataques terroristas de 1992 y 1994 en Buenos Aires).

Adicionalmente, en el año 2004, los medios masivos de comunicación de Perú publicaron varios escándalos de inteligencia (escuchas ilegales, venta de información clasificada por personal del servicio de inteligencia), los cuales llevaron a una reestructuración de la base ejecutiva y legislativa del sistema de inteligencia del Estado, y a nuevas regulaciones para el personal de inteligencia. En España, al igual que en Perú, iniciativas legislativas y judiciales han estado al tanto del activismo de los medios de comunicación, y una cultura de inteligencia y seguridad poco a poco ha surgido, encabezada por la comunicación del Ministerio de Defensa a la sociedad civil sobre el tema de inteligencia. Los autores concluyen, no obstante, que “mientras la percepción de inteligencia ha cambiado en el mundo académico, todavía tiene que cambiar entre los ciudadanos españoles”.<sup>14</sup>

En Portugal, la legislatura ha impuesto una separación de la producción de inteligencia del Estado preventiva sobre las amenazas internas, de la información de policía. La información de la policía es distinta porque aborda prevención de crímenes y la supresión de ellos con el uso de la acción policial. En la práctica, esta clara distinción no toma en cuenta una superposición de realidades actuales,<sup>15</sup> y no contempla nuevas aproximaciones de la inteligencia como es la inteligencia criminal. Sin embargo, la división permanece vigente para apoyar en las oportunidades del poder legislativo y judicial a distinguir actividades de inteligencia del Estado, las cuales operan en secreto y están sujetas a supervisión y control externo, del proceso criminal más transparente, lo cual involucra a los policías y las cortes. No obstante desconoce la dimensión aplicada de la actividad de inteligencia en materia de crimen organizado y las tendencias delictuales contemporáneas que pueden realizarse desde la función policial. Además, esta estrategia de gestión divisiva del tema limita el intercambio de información entre los servicios de inteligencia y la policía.

La cautela política respecto al mundo secreto de inteligencia, incorporado en las leyes, se extiende a no permitir a los servicios de inteligencia la conducción de la vigilancia o la interceptación de comunicaciones dentro de Portugal, una prohibición que posiblemente cambie con el fin de promover la credibilidad internacional de la inteligencia portuguesa ante los ojos de organismos extranjeros, los cuales desean colaborar en casos difíciles relacionados con la seguridad transnacional y la criminalidad.

## Gestión de Inteligencia en las Américas

Observamos en Portugal una sobrecarga de controles a las acciones de los servicios de inteligencia. Se presenta el desafío de encontrar un punto de equilibrio en la gestión de los controles externos, para que no impidan la eficacia de los servicios.

Otro aspecto que se relaciona con lo anterior es el concepto de la ética de inteligencia. El sentido ético de profesionales de inteligencia, por el cual decisiones reflexivas deben hacerse en asuntos tales como qué o quién debe ser objetivo de recolección, con cuáles medios, y bajo qué circunstancias, reina por definición donde las leyes y reglamentos específicos no determinan qué decisiones se deben tomar. El camino más claro para una ética de inteligencia justificable reside en la respuesta a la pregunta “¿Cómo está lógicamente relacionada la información que se busca con los principios (si hay algunos) enunciados en las existentes leyes y regulaciones de inteligencia?”<sup>16</sup> Si los principios no son apoyados, entonces la información no debe ser recopilada o buscada. En la ausencia de leyes relevantes o regulaciones en cada país, sólo la gama de pactos internacionales de derechos humanos menos específicos, convenios, y tratados están disponibles para invocarse.<sup>17</sup> A veces, aunque raramente, estos pueden ser sustitutos morales e incluso legales para directrices nacionales.

Desde esta perspectiva, vemos que si el gobierno fracasa en poner en marcha, y hacer cumplir, leyes y regulaciones apropiadas, entonces un funcionario de inteligencia tiene una gran responsabilidad de juicio en el desempeño de funciones que fácilmente pueden violar los derechos humanos, como se los definen en los códigos internacionales de conducta humana. Bajo un régimen de Estado de Derecho, existe un poderoso incentivo por parte de los expertos de inteligencia para apoyar la promulgación de leyes y regulaciones de inteligencia. Irónicamente, como varios autores han notado, cuando un profesional de inteligencia goza del respaldo de las leyes y regulaciones, es más probable que él o ella puedan cumplir sus tareas de una manera más agresiva.<sup>18</sup> Igualmente, podría atenuarse el entusiasmo para el cumplimiento de tareas si existiera en un determinado país una ley de inteligencia que estableciera transparencia al público sobre los detallados procedimientos de la función, hasta el punto donde los analistas o recolectores de datos prefiriesen elegir no aceptar el riesgo de tomar decisiones en este entorno de información típicamente incompleto.

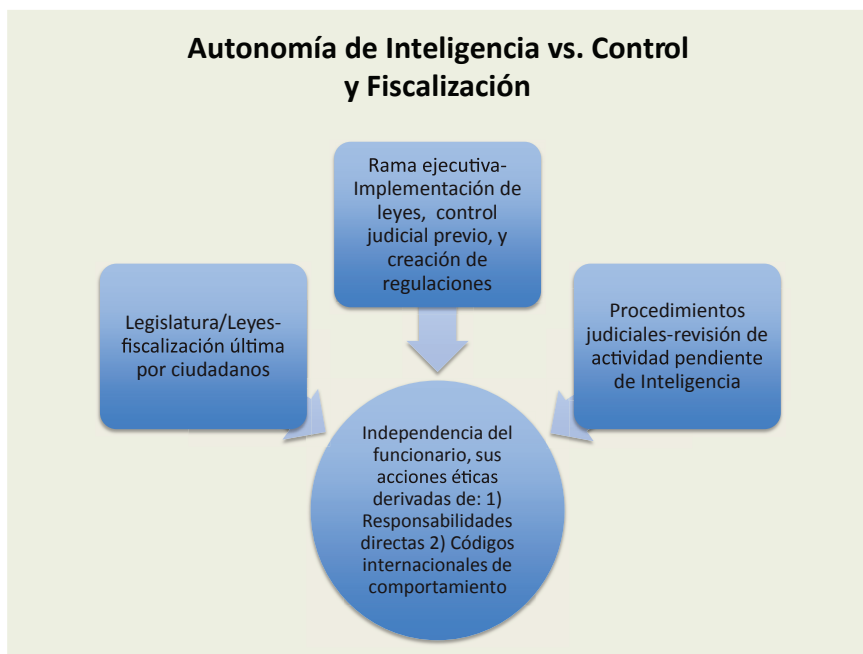


Figura 1. Fuente: Desarrollada por el autor.

El profesionalismo guiado por principios éticos constituye una razón para permitir cierto grado de autonomía en la toma de decisiones dentro de los servicios de inteligencia. Un grado apropiado de autonomía permite a un individuo o agencia construir una sólida reputación de independencia de criterio. El entusiasmo y criterio de un experto de inteligencia se aprecia a escala internacional por homólogos en otros países quienes son encargados de rastrear y neutralizar los objetivos, o recopilar pruebas en apoyo a su investigación, dependiendo de la orientación y prioridades de las organizaciones interesadas. Un resumen actual de la actividad de cooperación entre los servicios de inteligencia internacional explica que la colaboración de inteligencia está llegando a un nivel profundo de intercambio interpersonal por lo cual países con experiencia en la lucha contra amenazas internas, a menudo pasadas por alto en el pasado, se han convertido en los nuevos equipos de capacitación para otros que enfrentan desafíos similares.<sup>19</sup> Se puede agregar que el prestigio de sus servicios de inteligencia pueden convertirse en un indicador público del respeto y legitimidad—“ya sea positivo o no”—de una nación, particularmente

## Gestión de Inteligencia en las Américas

si los servicios de inteligencia del país o su “cultura de espionaje” llegan a ser representados en las películas populares.<sup>20</sup>

La gestión apropiada brinda el logro de confianza en los servicios de inteligencia de un país por parte de los poderes del gobierno más los ciudadanos, así como entre los observadores internacionales, y contribuye a la circunstancia ideal por la cual las mejoras en la efectividad y la eficiencia de actividades de inteligencia no disminuyan la aplicación individual o colectiva de los derechos humanos.

En resumen, prácticas apropiadas de gestión de inteligencia pueden ser de beneficio para todas las partes de esta función pública. Un observador políticamente orientado ha examinado los argumentos de las coaliciones a favor del orden y a favor de los derechos civiles en la región y sugiere que la inteligencia y los asuntos internos de la policía son áreas todavía sin reforma. Él pasa a explicar cómo las redes que promueven la movilización de la opinión pública pueden aprovecharse de los esfuerzos de reforma para establecer una mejorada rendición de cuentas por parte de los funcionarios de inteligencia y de la policía. Resulta que a su vez las operaciones de inteligencia y de policía pueden ser vistas más claramente en su rol de complementar la protección, en lugar de la disminución, de los derechos humanos individuales.<sup>21</sup>

La integridad de los expertos en inteligencia continúa siendo una preocupación, pero existe un control ejercido por los poderes legislativo, judicial y ejecutivo en países de la región para garantizar que la integridad sea reconocida y mantenida. Naturalmente, estos mecanismos no trabajan a la perfección, muy como los principios legales y éticos incorporados en leyes y regulaciones no son uniformes ni siempre o estrictamente aplicados. Para mantener la integridad de la fuerza laboral de los trabajadores o profesionales de inteligencia en su totalidad, de vez en cuando puede ser necesario revelar información sobre las prácticas ilegales dirigidas a autores independientes u organizaciones de comunicación masiva de modo que la presión pública pueda ayudar a conducir a los servicios de inteligencia a volver a utilizar prácticas autorizadas.<sup>22</sup> La divulgación de información confidencial no autorizada a la prensa ocurre ahora con una frecuencia suficiente para sustentar un proceso de revisión pre-publicación entre agencias del gobierno y empresas de los principales medios de comunicación.<sup>23</sup>

Otra manera en la que una persona “de adentro” puede cumplir con la responsabilidad de mantener la integridad de los servicios de inteligencia es publicar un relato de las prácticas reales ya sea en una novela de ficción, o como la premisa para una producción cinematográfica.<sup>24</sup> Este acercamiento a la narración de novelas de espionaje puede lograr la meta principal de educar al público, así como también informar a los funcionarios públicos con responsabilidades de supervisión y control, acerca de las motivaciones que conducen al cumplimiento y al no cumplimiento de las normas legales y éticas.

En la primera sección del libro, seis contribuciones esbozan los valores institucionales e incentivos personales que destacan la tensión existente entre el ámbito de la autonomía de inteligencia y el control del territorio o supervisión externa. Algunos autores exploran el difícil proceso de crear las leyes de inteligencia o mecanismos de control que respondan a los criterios de eficiencia, eficacia, legalidad y legitimidad, las cuales son un tipo de expresión del monitoreo externo, mientras otros autores señalan la importancia central y la viabilidad de la autonomía mediante una aplicación de la ética en el trabajo para funcionarios de inteligencia. Los autores también se dirigen a una reexaminación de los obstáculos que enfrentan las acciones de inteligencia que surgen de los procedimientos judiciales y de la percepción negativa por parte del público. Un comentario final sobre la responsabilidad de los medios de comunicación de cambiar el foco de su atención desde aspectos operacionales de inteligencia gubernamental hacia el rol legítimamente estratégico sirve de transición a la próxima sección.

## 2. Gestión de inteligencia dentro del poder ejecutivo del gobierno

*Concepto clave: Efectividad de la información académica y de otras fuentes de información empresarial vs. efectividad de los servicios militares y civiles profesionales en asesorar a líderes democráticos*

Aunque un típico comandante militar considera que la inteligencia será un aporte confiable para la toma de decisiones, un líder civil en una democracia aprende a confiar en los asesores que le han ayudado a él o a ella a ganar la elección. Sin la oportunidad de construir confianza con el nuevo líder político antes de la elección, los servicios de inteligencia de un país pueden estar en desventaja para ganarla incluso luego de la elección. Esta idea es reforzada por la investigación de un científico político.<sup>25</sup> En su investigación, le fue posible

## Gestión de Inteligencia en las Américas

obtener información de un instrumento de encuesta presentado a funcionarios del gobierno en EE.UU. y Reino Unido. Sus resultados mostraron que en ambos países, la información de fuentes no gubernamentales es utilizada con la misma frecuencia que la información gubernamental, inclusive en la toma de decisiones relacionadas con la política exterior del país. En contraste, un autor israelí sostiene que líderes políticos y regímenes democráticos tienden a confiar en las evaluaciones de sus servicios de inteligencia para la toma de decisiones con respecto a los asuntos internacionales.<sup>26</sup> Sin embargo, estos estudios no son claramente aplicables a las decisiones de seguridad interna, en donde se escucharán muchas más voces de toda la sociedad, y donde los asesores de inteligencia pueden carecer de la combinación de objetividad y experiencia para hacer notable su propia voz.

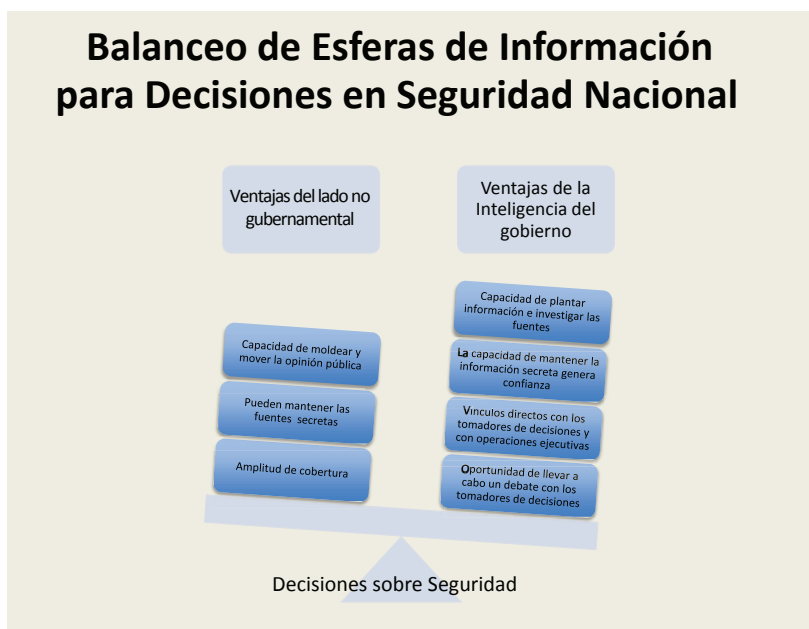


Figura 2. Fuente: Desarrollada por el autor.

Otro documento, de fecha más reciente, sugiere que el restringido punto de vista típico de los especialistas del gobierno, quienes simplemente carecen del tiempo para absorber el flujo de fuentes abiertas de información además de



los muy valiosos datos disponibles de fuentes secretas, no les permite “clarificar asuntos tales como el cambio de clima, seguridad energética, estabilidad financiera global o seguridad alimentaria”.<sup>27</sup> El autor de este documento reafirma que los principales líderes políticos tienden a no incorporar la *evaluación* de los servicios de inteligencia del gobierno en su forma de pensar; al contrario, ansiosamente miran a elementos secretos fragmentarios y “prefieren el drama y la claridad de un reporte de una sola fuente a los matices cuidadosos” de evaluaciones balanceadas ofrecidas por analistas del gobierno.<sup>28</sup>

Si se trata un producto estratégico de un cuerpo formal de profesionales de inteligencia, o de diplomáticos, las evaluaciones sustantivas realizadas por los servicios de inteligencia del Estado probablemente tiene mayor peso que los juicios, opiniones, y recomendaciones muy bien sustentadas, de periodistas, especialistas de centros de estudios, y tal vez de los amigos de confianza de esos quienes toman decisiones políticas. Existen factores importantes los cuales permiten a los profesionales de inteligencia y sus contribuciones diferenciarse de las de sus colegas académicos especializados y bien posicionados. Uno es generalmente su acceso directo a aquellos que toman decisiones y forman políticas, junto con acceso a los civiles o militares que implementan la política elegida;<sup>29</sup> otro es su acceso a fuentes de información secreta, y su disposición a proteger lo secreto, así ganando la confianza de quienes toman las decisiones.

Adicionalmente, por virtud de las capacidades del servicio de inteligencia, sus funcionarios pueden esperar reunir información bajo condiciones encubiertas o clandestinas para confirmar, o preferiblemente, refutar una hipótesis. Esta capacidad incluye la oportunidad de colocar información falsa que podría conducir al blanco de la inteligencia a revelar sus verdaderas intenciones. Finalmente, los decisores generalmente buscan una garantía de que no habrá fuga de información confidencial por parte del profesional de inteligencia, una garantía la cual no es difícil cumplir por los profesionales de inteligencia, porque ésta es una característica principal de los expertos que trabajan en inteligencia.

La gestión de inteligencia es caracterizada por varios temas. Uno de ellos es la naturaleza de la relación entre el más alto funcionario electo de un gobierno en particular y el personal de inteligencia que ofrece sus evaluaciones, prospectiva y juicios en asuntos clave. Es decir: ¿Debería el personal de

## Gestión de Inteligencia en las Américas

inteligencia intimar con el funcionario al que informan o asesoran hasta el punto de tener empatía con esa visión del mundo del funcionario y del tema que los preocupa? O por el contrario, ¿Deberían mantener una distancia psicológica y política del funcionario? Podemos suponer que cuando cierta distancia es mantenida, un profesional de inteligencia es menos propenso a conspirar contra el funcionario público.

Empero, algunos observadores estadounidenses e incluso algunos profesionales de la inteligencia recomiendan no mantener una distancia del funcionario a cargo de decidir sobre la política o acción del momento. El bien conocido Robert Gates, después de ser Director de la Agencia Central de Inteligencia y Secretario de Defensa, escribió sus experiencias como Asesor de Seguridad Nacional para el Presidente George H.W. Bush. Él descubrió que la tendencia del personal de la Comunidad de Inteligencia para mantener una distancia psicológica de los funcionarios de la Casa Blanca no logró los resultados que debían ser alcanzados.<sup>30</sup> Muchos oficiales de inteligencia consideran que “trabajar de modo demasiado cercano” con altos oficiales que toman decisiones políticas (es decir, toman en cuenta sus metas políticas) puede llevar a ajustes por parte del uno o del otro a los asesoramientos, o a una búsqueda de información predeterminada para justificar una política ya decidida—la esencia de la llamada “politización”. Pero desde una aplicada perspectiva académica, Richard Betts evalúa los beneficios y costos de la politización, la cual para él sale beneficiada cuando la inteligencia “no representa falsedades pero a la vez presenta la información de una manera que impide que sea dejada a un lado como irrelevante”.<sup>31</sup> Para alimentar la utilidad del producto de inteligencia, el autor Woodard recomienda que sus practicantes no la consideren simplemente como “información sustentadora” pero neutral respecto a las políticas, sino que reconozcan el rol directo de la inteligencia en conferir a los que toman decisiones una “ventaja decisional”. La inteligencia presenta una ventaja para el oficial que toma decisiones cuando el producto resultante es persuasivo. Un informe con factores persuasivos se caracteriza en incluir una argumentación soportada con evidencias, junto con una retórica y elocuencia responsable.<sup>32</sup>

Dos autores, oficiales del gobierno de EE.UU., explican por qué el modelo de la inteligencia orientada a tomar en cuenta el ambiente político de los que toman decisiones no debe ser rechazado. Kerbel y Olcott reconocen la idea de que oficiales de alto nivel utilizarán cualquiera de las fuentes de información,

muchas de ellas por fuera del gobierno, pero que de hecho estos oficiales a menudo dan la bienvenida a los juicios de inteligencia que son presentados personalmente y que se atreven a recomendar una política con respeto a los asuntos en cuestión. Además, nos informan que esta tendencia se extiende hasta el punto de escuchar la visión de los profesionales de inteligencia acerca del posible resultado de la acción recomendada.<sup>33</sup>

Este punto de vista es exactamente el opuesto a la tradición de la Comunidad de Inteligencia de los EE.UU., originalmente promovida por Sherman Kent, de mantener una distancia intelectual entre el juicio de una inteligencia “pura” y el mundo político, en el cual personal de la inteligencia no debe ser involucrado. El enfoque propuesto por Kerbel y Olcott, que hasta la fecha no es empleado plenamente en la Comunidad, podría provocar un cambio fundamental en la manera que el personal de inteligencia se aproxima a los principales funcionarios que toman decisiones en los EE.UU. Aunque estos dos autores no lo mencionan, hoy la Comunidad de Inteligencia está intentando una nueva manera para dirigir la interacción personal entre los profesionales de inteligencia y los oficiales principales responsables de las decisiones de política nacional.<sup>34</sup> La nueva técnica es llamada “exposición con confrontación”, la cual cuenta con el objetivo de mejorar la comunicación entre el funcionario de inteligencia y el oficial responsable. La misma consiste en una serie de reuniones asistidas por los funcionarios y un oficial, donde dos funcionarios de inteligencia toman posiciones contrastadas sobre un tema de interés, en un formato de debate. En resumen, esta otra técnica provee al personal de inteligencia una decisiva ventaja sobre las fuentes de información que compiten en términos de su influencia potencial en decisiones o acciones políticas relacionadas con la seguridad.

El fenómeno económico ciertamente juega un papel en la seguridad nacional, y por lo tanto, como preocupación va aumentando en la inteligencia.<sup>35</sup> Las amenazas y oportunidades económicas ilustran muy bien la idea de que pocos sectores en un país pueden escapar una influencia extranjera fuerte. La globalización significa que la influencia extranjera es manifestada internamente y es por lo tanto un blanco doméstico adecuado para las capacidades de inteligencia del Estado. La incorporación de evaluaciones financieras en el repertorio de las capacidades de inteligencia nacional hasta ahora se ha enfocado en el crimen organizado, sobre todo porque su actividad se manifiesta con el lavado

## Gestión de Inteligencia en las Américas

de dinero. En varios países de la región, vemos ya a las Unidades de Inteligencia Financiera del Grupo Egmont, una entidad internacional no gubernamental.<sup>36</sup> Pero la difusión de delitos financieros y las amenazas económicas de carácter más general señala que habrá un valor indudable en el desarrollo de células del gobierno especializados en inteligencia o en equipos con esta orientación.

Como ha señalado un analista de Francia, un gobierno nacional es el último guardián contra las amenazas económicas, aun en países miembros de alianzas económicas formales o multilaterales.<sup>37</sup> Existe un modelo sugerente de cómo los profesionales de inteligencia, como especialistas en el fenómeno económico, pueden ser capaces de inferir o imaginar las bases del desarrollo económico en cualquier escala, y sus implicaciones para la seguridad nacional. Este modelo nos familiariza con una serie de eventos históricos que desde el punto de vista de hoy en día creó la forma fundamental de la actual situación geoeconómica a nivel mundial.<sup>38</sup>

¿Sería posible para los funcionarios del gobierno responsables de la evaluación de la inteligencia económica identificar los eventos que en el curso de la “historia futura” sean de importancia trascendental a nivel nacional? o, en forma alternativa ¿Es necesario contar con evaluaciones y prospectiva hechas por expertos del sector financiero? Al respecto, tenemos la opción de adoptar una gestión administrativa que emplea reconocidos expertos en los rangos de funcionarios de inteligencia del gobierno quienes trabajan, e incluso crean, oficinas o agencias adecuadas, y quienes están dispuestos a participar permanentemente en análisis de inteligencia económica, como una especie de prueba de su lealtad para el bienestar del Estado y los ciudadanos.

Indudablemente, los líderes de un gobierno pueden buscar asesoría política en asuntos de seguridad y defensa doméstica e internacional en cualquier parte, y sus servicios de inteligencia deben competir por la atención de los decisores políticos junto con otros proveedores de información y asesoría acerca de las implicaciones generadas por las opciones políticas. Con suficiente apoyo político, un gobierno democrático también puede reducir o aumentar los recursos disponibles para financiar actividades de inteligencia. Sin embargo, un enfoque de la gestión de inteligencia que asegure la habilidad de análisis a largo plazo para entender los asuntos económicos, por ejemplo, y para evaluar el valor de la inteligencia del manejo y explotación de información de fuentes abiertas a gran escala, sería una buena inversión en las instituciones que por

definición tienen los intereses del Estado como valor central, como tiene el conjunto de servicios de inteligencia de un país.

La ausencia en los últimos años de un masivo despido de los funcionarios es un indicador positivo de una gestión prudente. Esta historia reciente se contrasta con la historia menos reciente que incluye el despido imprudente de personal de inteligencia experimentado en varios países de la región mientras los nuevos gobiernos ejercieron su poder para ajustar la estructura burocrática. Estos abruptos ajustes al personal de inteligencia se han llevado a cabo en los Estados Unidos, Argentina, México, Perú y Colombia y en su momento ciertamente redujo la amplitud de las experiencias de los individuos que en su conjunto normalmente crean un importante conocimiento institucional.<sup>39</sup> Al final, la utilidad de los servicios de inteligencia, los cuales presentan ventajas de información sobre fuentes alternativas de información privada, exigen atención del Poder Ejecutivo para asegurar un entendimiento exhaustivo y corporativo de asuntos de seguridad y de los medios para dirigirlos a través de fuentes responsables del gobierno.

Los cuatro ensayos de la segunda sección del libro investigan las oportunidades para la gestión de inteligencia desde el punto de vista de funcionarios del poder ejecutivo en las Américas. Se indica por cada autor de la sección cómo los recursos nacionales de inteligencia pueden insertarse en el tejido de la seguridad ciudadana, vía decisiones ejecutivas que tomen en cuenta las capacidades del personal de agencias de inteligencia, junto con los programas ahora existentes, o a desarrollar.

### **3. La gestión en asuntos de privacidad y seguridad en la comunidad de inteligencia**

*Concepto clave: Uso de inteligencia policial vs. instituciones nacionales de inteligencia para abordar asuntos internos de seguridad*

En los últimos años, la adopción de métodos de inteligencia por parte de las fuerzas del orden público ha aumentado, y se ha convertido en una herramienta para la prevención del crimen. Entre las razones para el enfoque en la prevención del crimen, es notable que las actividades delictivas se estén convirtiendo en un fenómeno menos casual y a menudo más organizado y producto de grupos criminales que traspasan las fronteras nacionales.

## Gestión de Inteligencia en las Américas

La naturaleza de la organización de los grupos delictivos implica que sus actividades sean planificadas, una tendencia que ofrece una apertura para el empleo de métodos preventivos por parte de la policía.

Las mismas motivaciones y tendencias que han resultado en una gama cada vez mayor de entidades de inteligencia gubernamental, pueden crear obstáculos a largo plazo para la integración de la comunidad de inteligencia. Por ejemplo, en los Estados Unidos pos-9/11, más allá de la creación del Departamento de Seguridad Nacional y la expansión de la Comunidad de Inteligencia Federal, las ciudades de New York, Dallas y Los Ángeles han desarrollado capacidades notables de inteligencia, con la aplicación de un enfoque preventivo similar a la del gobierno nacional, pero sin ninguna colaboración de las agencias nacionales de inteligencia.<sup>40</sup> En un ambiente de recursos abundantes, la tendencia, por lo tanto, ha sido una multiplicación de organizaciones de inteligencia, motivadas por la idea de que existió una falta de capacidad dedicada a la recopilación de información relevante sobre las necesidades locales en un sentido burocrático o geográfico.

En combinación con la expansión de agencias de inteligencia del gobierno en los Estados Unidos, hemos visto la continuidad de un percibido “muro” que ha prohibido el intercambio de información y evaluaciones entre el mundo de la inteligencia policial e inteligencia de seguridad nacional.<sup>41</sup> Certificado por autores con amplio conocimiento, este muro divisorio, en efecto, no existió como una barrera legal para el intercambio de información o inteligencia.<sup>42</sup> Este fue, y es, en efecto, un producto de la naturaleza política de la función de inteligencia. Desde el comienzo de la “guerra contra el terrorismo”, en los casos que ha habido un error de omisión, como lo hubo antes del 9/11, líderes de inteligencia y observadores externos por igual prefieren culpar al “sistema”, en vez de responsabilizar de los errores a individuos o agencias de inteligencia. Si existe un problema con respecto al sistema de inteligencia, entonces hay algunas preguntas a ser respondidas sobre cómo el sistema opera. Por ejemplo, en vista de la separación entre el lado de seguridad policial y el terreno de la seguridad nacional, ¿Cómo puede ser integrada la inteligencia a nivel nacional a la información obtenida por la policía? ¿Son los intercambios informales entre profesionales de inteligencia suficientes para superar los elementos de división que impiden la eficiencia potencial y esperada de la profesión de inteligencia al realizar estas tareas?

Una respuesta inicial y positiva es ofrecida en un reciente libro escrito por un oficial de policía diplomático.<sup>43</sup> Él explica que las fuerzas del orden público de países en el mundo actualmente y a menudo están de acuerdo en compartir información local con sus homólogos de otros países si esta información es de valor para la inteligencia del Estado o para fines acusatorios. Ahí existe incluso un alto grado de cooperación, en ciertos casos, entre la policía diplomática de EE.UU. y la policía local de otros países hasta el punto que los oficiales locales pueden decidir en compartir información sin obtener aprobación previa de los oficiales nacionales.<sup>44</sup> Existe este escenario debido a la distancia política generalmente mantenida entre la policía local y las autoridades nacionales.

Pero, ¿qué sabemos de la existencia y consecuencias de este tipo de compartimentación de información dentro de un determinado país? Y, dados los intercambios de información que se producen, ¿cómo podemos desarrollar y manejar una estructura de información y una disposición de inteligencia del gobierno que logre tomar mayor ventaja institucional de relaciones informales y personales entre el personal de organismos de inteligencia? Es decir, ¿cómo podemos construir instituciones para promover los intereses internos y externos de un país por medio de un intercambio informal de información de seguridad para luego crear productos de inteligencia?

Una respuesta en forma de innovación institucional, parece ser encontrada en las fuerzas híbridas (de perspectiva nacional y internacional, pero con poderes policiales) de orden público que cuentan con misión de seguridad interna desde la perspectiva policial, con plena atención de la administración judicial de leyes civiles a los derechos humanos. En los Estados Unidos, esta innovación se ve en la *Coast Guard*, y en Argentina, la Gendarmería Nacional.<sup>45</sup> Sin embargo, la policía local y sus capacidades de inteligencia operan principalmente con base en la inteligencia humana, en vez de una disciplina de recopilación más técnica como la inteligencia de señales o la inteligencia de imágenes, y sirve primariamente a las necesidades locales. Por lo tanto, a pesar de que puede haber la necesidad de información nacional para combatir la actividad criminal transnacional que tiene expresión local, hay poco incentivo por parte de una organización nacional de inteligencia en compartir su información con fuerzas policiales locales porque generalmente la policía nacional no recibe datos sobre asuntos de interés de la policía local que podrían a la vez ser de interés nacional.<sup>46</sup>

## Gestión de Inteligencia en las Américas

De hecho, una presencia amplia y profunda de una institución de policía nacional sería necesaria para coordinar y actuar sobre la información recopilada en todo lo ancho de un país. Tal presencia de la fuerza de policía nacional puede recordar a los residentes del desprestigiado enfoque de “seguridad nacional” adoptado por gobiernos autoritarios anteriores, aunque el modelo de policía nacional se aplica principalmente a países unitarios, y no tanto a países federales. En sociedades democráticas, la “seguridad nacional” a menudo no se le asigna un alto valor por parte de los ciudadanos, ya que es algo alejado de la vida cotidiana y también algo sobre lo cual tienen poco o ningún poder.<sup>47</sup> Especialmente en gobiernos autoritarios recientes, el concepto de una policía nacional está destinado a tener asociaciones negativas. ¿Es posible que un marcado aumento en los recursos de inteligencia para la policía regional y municipal, en un paradigma descentralizado de recopilación de información y regulación, permita la construcción de capacidades para abordar la criminalidad nacional o transnacional, y así reducir las preocupaciones de los ciudadanos acerca de sus similitudes con la policía política de la “Seguridad de Estado”?



Figura 3. Fuente: Desarrollada por el autor.



El esquema ilustra las ventajas comparativas para la seguridad del ciudadano ofrecidas por la policía nacional o servicios de inteligencia que se involucran en garantizar la seguridad interior. Cada uno de los cinco puntos de comparación es presentado en el mismo orden en cada columna. Como comentario en el último de los cinco puntos, la participación desde el nivel nacional en los asuntos locales es a menudo poco grata, sin embargo, una adhesión visible a las normas internacionales, en las acciones de las fuerzas de seguridad nacional, les ayudarían en ganar o mantener una percepción pública positiva en el ambiente internacional.

La policía local guiada por la inteligencia, conocida por los profesionales de seguridad como “policía comunitaria”, puede generar información de inteligencia para la seguridad interna al “por menor”.

Hoy en día, los defensores de la reforma policial a través de América Latina tratan de responder a demandas de seguridad pública mediante la promoción de modelos de policía comunitaria. Aunque están poco adaptados para llevar a cabo el trabajo pesado que requiere la lucha contra organizaciones criminales transnacionales, dichos defensores argumentan que la policía comunitaria ayuda a desmilitarizar, democratizar, y descentralizar a instituciones del orden público, poniendo un énfasis operacional en el juicio de los agentes en el campo y mayor control sobre el uso de fuerza.<sup>48</sup>

El desarrollo de inteligencia preventiva también implica que será utilizada para algún propósito, y la policía local podría perder la confianza en comunidades a las que sirve si la información se añadiera a una base de datos criminales a nivel nacional, por ejemplo, en vez de ser utilizada para el claro beneficio de los locales. Esta perspectiva puede ayudar a explicar el por qué bases de datos nacionales, tales como la Plataforma México y el Sistema Nacional de Información de Justicia y Seguridad Pública (INFOSEG) de Brasil, han demorado en incorporar información de la policía local u otras organizaciones de seguridad. No obstante, mientras la criminalidad local se fusiona cada vez más con empresas criminales a escala nacional o internacional, también aumentan las oportunidades para que la inteligencia regional o de ciudades sea institucionalizada. Un caso a señalar proviene de México, y en particular del estado del noreste Nuevo León, en donde la ciudad capital es Monterrey.

## Gestión de Inteligencia en las Américas

Según indican unos observadores mexicanos, el estado mexicano de Nuevo León recientemente adoptó una ley que específicamente penaliza la actividad de los “halcones” empleados por organizaciones de tráfico de drogas para espiar la actividad de policías y militares que puedan poner en peligro la libertad de acción de los traficantes.<sup>49</sup> La estructura federal del gobierno Mexicano ofrece a cada estado de la federación la oportunidad de aplicar y adaptar leyes similares para reducir la impunidad de al menos ciertos individuos. Esta medida legal tiene como objetivo los “empleados” locales de organizaciones traficantes, y señala una notable intervención de la comunidad en el Estado de Derecho. En la medida que esta ley y otras parecidas recaen sobre los delincuentes puede ser monitoreada para determinar si la regla fundamental del Estado de Derecho está siendo aplicada a la vida diaria de la comunidad en donde la seguridad de los ciudadanos está en balance.

Una preocupación seria es que la policía comunitaria, incluida la policía guiada por la inteligencia, está particularmente sujeta a la influencia política local, o lo que podría llamarse “corrupción”.<sup>50</sup> Un destacado experto en policía comunitaria de América Latina explica cómo sucede esto:

Iniciativas de seguridad basadas en los ciudadanos con frecuencia son arregladas por los propios ciudadanos. Las juntas de vecindarios y patrullas llegan a ser cooptados por los comisionados del vecindario, por traficantes de droga, o por directores de programas quienes canalizan fondos a sus amigos... La mayoría de las comunidades son deficientes en la cohesión, finanzas, y experiencia necesitada para formar grupos durables que puedan identificar consistentemente las causas de la inseguridad—a no mencionar romper las condiciones donde prevalecen el miedo, desconfianza, y violencia que caracterizan las relaciones de ciudadanos con la policía. A la medida que las tendencias económicas continúan a poblar las áreas urbanas pobres con recién llegados, hasta los vecindarios establecidos experimentan dificultad en mantener organizaciones comunitarias, y resulta que encontramos un límite al conocimiento e información que llega a la policía.<sup>51</sup>

En un ensayo anterior, el mismo autor afirma que en la Ciudad de México, completamente el 70% de la policía está asignada a proteger negocios, en

lugar de actuar como autoridades locales de gobierno y del público mediante una ronda de patrullaje en espacios públicos.<sup>52</sup> En una nota relacionada, otra veterana observadora de las tendencias de justicia criminal en la región señala que en Argentina, el tema de su estudio, los espacios públicos y urbanos no patrullados, fuera de las “comunidades cerradas”, continúan creciendo en tamaño y en violencia.<sup>53</sup> A la luz de estos hallazgos, al grado de que son representativos en la región, la falta de presencia policial en espacios públicos y “zonas peligrosas” de comunidades urbanas que son “propiedad” de elementos criminales, en fin ofrece pocas oportunidades e incluso menos incentivo para la policía local en áreas urbanas para que éstos recopilen información útil para la prevención o para enjuiciar a los criminales. Estas observaciones, en conjunto con la cooptación política de actividades policiales en ciudades y provincias individuales como se señala en el material citado anteriormente, reduce la voluntad de la comunidad para proveer información a la policía. A menos que el activismo judicial como es visto en Nuevo León, México, se haga más generalizado y eficaz, no se debe esperar de la policía local que contribuya de una manera significativa a la mejora percibida o real de la seguridad interna o su par, la seguridad ciudadana.

Uno puede imaginar que las ciudades más grandes de la región podrían tener la magnitud de los recursos y visibilidad pública para promover una iniciativa de policía basada en la inteligencia eficaz, si no eficiente. Sin embargo, fuera de la muy publicada fuerza de inteligencia de New York,<sup>54</sup> con su alcance internacional, y el éxito limitado retratado en la popular serie de películas brasileña *Tropa de Elite*, que muestra en gran parte el empleo y el manejo de inteligencia policial en Río de Janeiro, aún no existen muchas pruebas de que las fuerzas del orden público urbano hayan alcanzado el nivel de profesionalismo de inteligencia o integridad que ya se espera de las fuerzas policiales nacionales o federales. La ciudad de New York probablemente tenga el establecimiento de inteligencia policial más amplio y notorio de cualquier ciudad en el hemisferio, pero sus críticos observan que tiene poca capacidad para el análisis, y en contraste con agencias nacionales de inteligencia, sólo cuenta con una guía *ad hoc* respecto a la información a recopilar.<sup>55</sup> El desenfrenado enfoque de esta ciudad hacia la recopilación de información por su División de Inteligencia ha sido difundido ampliamente al público y fuertemente criticado por organizaciones de los derechos humanos así como por la Oficina Federal de Investigaciones [FBI].<sup>56</sup> Las operaciones domésticas del FBI, en

## Gestión de Inteligencia en las Américas

contraste con aquellas de la policía de la ciudad de New York, deben observar estrictas normas de libertades civiles.<sup>57</sup>

Al anticipar la tercera sección de este libro nuestro objetivo ha sido examinar algunos de los factores que afectan las capacidades de inteligencia de la policía local o urbana, y contrastar aquellos con capacidades de instituciones de inteligencia del Estado para abordar la seguridad interna o seguridad ciudadana en el entorno globalizado contemporáneo. En la primera sección del libro en donde contrastamos el valor de la autonomía de la inteligencia con relación a la supervisión y requisitos de responsabilidad, constatamos que Portugal ha separado a la inteligencia policial de la inteligencia de seguridad nacional para propósitos de supervisión, pero con un limitado éxito funcional y de gestión. En el presente ensayo, vemos que la policía guiada por la inteligencia a un nivel sub-nacional, aun cuando cuenta con los recursos necesarios, puede inspirar desconfianza entre los ciudadanos cuya seguridad puede tener un costo representado en la falta de libertades civiles. Las fuerzas del orden público nacionales o internacionales son más adecuadas para abordar actividades del crimen organizado con sus robustas capacidades de inteligencia, pero aun así pueden ser los sustitutos inadecuados para las capacidades locales de la policía por la percepción de los ciudadanos de su similitud con la “policía política” de regímenes autoritarios anteriores.

Estos hallazgos dejan otra opción de gestión de inteligencia internamente enfocada para asegurar la seguridad del ciudadano. Esta opción abarca una combinación de responsables sobre las capacidades técnicas o de una “inteligencia social” de la inteligencia militar nacional que podría ser aplicada bajo excepcionales circunstancias en colaboración con el detallado conocimiento local de oficiales políticos o de la policía. Este enfoque se explora en el ensayo sobre México en esta tercera sección del libro. Otro ensayo de la sección aborda la necesidad de generar inteligencia en el sistema de prisiones de un país, en donde uno podría esperar obtener perspectivas útiles sobre cómo operan las compañías del crimen organizado. Nuevamente, una combinación de recursos de inteligencia del Estado y la familiarización de la policía local con las características de la franquicia criminal podrían aprovechar mejor las oportunidades de recopilación y utilización de información obtenida en instituciones penales. Finalmente, esta tercera sección del libro destaca un ensayo que esboza la influencia perdurable de

las instituciones de la inteligencia militar en Brasil, en una manera que nos recuerda los obstáculos que se presentan en el logro de la integración de una inteligencia civil o paramilitar (de policía) que a la vez se hace de modo responsable—bajo la supervisión democrática del tema.

#### 4. La gestión de una integración de la inteligencia: un desafío de los servicios de inteligencia

*Concepto clave: El intercambio de la información a través de todas las instituciones del Estado y desde los ciudadanos, permite la integración de “conocimientos profundos” de los funcionarios de inteligencia junto con los valores de la sociedad. Esta situación ideal se promueve mediante una robusta educación profesional en inteligencia, la colaboración pública/privada en el contexto del ciberespacio, y por un experimento de campo en el área de asesoramiento a altos oficiales en un ámbito de compartimiento de información, dentro de un escenario de enlace multilateral.*

La integración de inteligencia generalmente se concibe como un estado ideal de colaboración y cooperación entre instituciones de inteligencia o aceptado libremente o percibido como un mandato de los distintos organismos, oficinas o agencias que forman un sistema o comunidad de inteligencia. Pero esta visión restringida del fenómeno de integración oculta una concepción más amplia que considera a la integración como la reunión de capacidades de inteligencia junto con otros flujos de información que en su totalidad crean un clima de toma de decisiones y acciones positivas en el tema de seguridad a través de toda la sociedad. Aceptar esta visión amplia del rol de “inteligencia” en la sociedad, también precisa reconocer que la creación y maduración de ella se forma mediante iniciativas de los servicios de inteligencia junto con el apoyo de la autoridad política.

La característica tradicional de los servicios es limitar el acceso a información protegida a un grupo pequeño de personas—los funcionarios—que aceptan la realidad que son ellos mismos objeto de monitoreo, respecto a sus intenciones de mantener las normas de confidencialidad. Realmente, son estos funcionarios quienes tienen la libertad y responsabilidad de tomar las decisiones diarias sobre qué monitorear y compartir con otras entidades, dentro del flujo amplio de información, bajo condiciones de cumplir con las leyes y reglamentos vigentes. Mandatos legislativos y ejecutivos sobre la “responsabilidad de

## Gestión de Inteligencia en las Américas

compartir información con otras entidades” típicamente emergen solamente después de algún fracaso notable de inteligencia, especialmente una falta de identificación y prevención de un evento que tiene importancia política.<sup>58</sup>

Los tres ensayos de esta sección dan indicaciones de cómo los directores del sistema o comunidad de inteligencia, pueden hacer sus aportes con sus propias acciones de gestión, atribuciones y competencias a la seguridad y defensa de la nación. Se ve por las perspectivas y vivencias de los autores, que los servicios de inteligencia pueden superar los límites tradicionales de inteligencia para así promover el bienestar de la sociedad.

Los servicios de inteligencia del Estado a menudo tienen una institución—una escuela civil, a nivel de posgrado—que es la única en permitir a expertos dar un paso atrás para ver de nuevo y desde una distancia los detalles de su trabajo diario para contemplar el lugar de la inteligencia en su sociedad y cómo mejorar su funcionamiento. Parece que las instituciones educativas de inteligencia pueden influenciar, a través de su currículo y las habilidades del cuerpo docente, a otras instituciones de inteligencia más grandes tales como las ramas de inteligencia de las Fuerzas Armadas y los servicios civiles de inteligencia de un Estado. Es decir, las escuelas no sólo reflejan las experiencias de los estudiantes y sus organizaciones de origen. En su mejor momento las escuelas imaginan e iluminan el fenómeno social y técnico de inteligencia del Estado a partir de una perspectiva amplia e incluso teórica, siempre con la intención de llevar a cabo una investigación empírica y aplicada. También es un lugar donde se puede abordar y colaborar en la internalización de una formación ética para el profesional de la inteligencia.

Sabemos que las escuelas de inteligencia del Estado, ya sean civiles o militares, tienen una larga historia en algunos países.<sup>59</sup> También percibimos que en muchos países de la región, expertos en inteligencia de países amigos asisten a clases e incluso participan en su totalidad en los programas de las escuelas de inteligencia.<sup>60</sup> Una cosa que no se conoce, pero que al mismo tiempo puede ser percibida, es la naturaleza y la extensión de interacción personal y profesional en las escuelas de inteligencia que regularmente son anfitriones de estudiantes extranjeros. Por lo tanto, puede ser que en estas escuelas veamos desarrollándose, para alumnos de hoy igual que para los egresados de años anteriores, el fenómeno de una cooperación o integración de inteligencia que promueve ideas sobre cómo debe gestionarse esta función gubernamental en

la región. Como se destaca en el ensayo sobre la educación en inteligencia, existen varios casos de escuelas nacionales en la región donde se matriculan alumnos provenientes de variados sectores de la sociedad, junto a individuos con especializaciones en leyes, en asuntos comerciales así como en ocupaciones académicas.

La seguridad cibernética es dominio natural de los servicios de inteligencia, ya que la seguridad e integridad de gran parte de la actividad económica contemporánea, como también lo relacionado con las capacidades en defensa, dependen de la invulnerabilidad de comunicaciones digitales. La estructura de instituciones dedicadas a esta esfera, que son relativamente nuevas en términos de actividad de inteligencia, requiere de una estrategia para blindar la seguridad de una amplia gama de actividades económicas en un determinado país, tanto como mantener la seguridad cibernética de sus instituciones defensivas, frente a intrusiones y ataques cibernéticos. Hasta la fecha no existe esta capacidad por parte de un sistema de inteligencia en ningún rincón de la región. Debido a la naturaleza holística de las responsabilidades de desartar acciones preventivas en el área, la seguridad cibernética ofrece un terreno fecundo para la integración del sector privado con las capacidades del sector público, junto con una combinación de las competencias de expertos civiles y militares.

Podemos suponer que en el ámbito donde la privacidad es más valorada y esperada como un derecho humano, específicamente en comunicaciones privadas y familiares, hay ahora una mayor vulnerabilidad en la pérdida de la privacidad. Aunque podemos encontrar consuelo en culpar a los fisgones del gobierno por la pérdida de privacidad en comunicaciones personales, claramente Facebook, Google y otras redes sociales tienen la mayor oportunidad y también quizás el mayor incentivo para tomar ventaja de la información personal para su propio beneficio.

Al mismo tiempo, una interceptación menos acentuada por parte del gobierno de comunicaciones privadas es vista como una amenaza mayor, y sí se puede decir que el gobierno cuenta con poderes de coerción sin igual.<sup>61</sup> El uso continuo de servicios tales como Facebook y Google por millones de usuarios sugiere que el beneficio obtenido en la fácil forma de la recopilación de información personal tiene más peso que cualquier preocupación sobre el monitoreo de su mundo privado. Aunque una invasión de la privacidad

## Gestión de Inteligencia en las Américas

personal puede ser rechazada por ser sin justificación por algunos, los servicios de inteligencia de cada país se enfrentan con el reto de continuar su trabajo. Aún dada la posibilidad de una colaboración entre los servicios de inteligencia y las empresas de comunicación de un determinado país, si los servicios de inteligencia pueden demostrar su integridad ética y legal, al incluir su independencia legalmente respaldada frente a autoridades políticas, como se sugiere en el ensayo sobre ciber seguridad del presente libro, debe ser menos complicado para convencer a los ciudadanos de que su trabajo “sin fines de lucro” promueve el beneficio de la seguridad pública y ciudadana.

El transcurso de la integración de la inteligencia ha alcanzado un punto de inflexión notable cuando sus practicantes se encuentran en pleno trabajo sin poder ni tener que aplicar el término “inteligencia” para identificar la naturaleza de sus actividades y responsabilidades dentro de la administración pública. En el caso estadounidense, ha emergido este salto evolutivo debido a la implementación de la política internacional que aborda contribuciones entre la variada gama de agencias del gobierno, que es llamado *Smart Power*, innovación destinada a lograr un balance de influencias militares y no militares. Bajo este régimen, los objetivos de la política exterior en un entorno de colaboración para el desarrollo de instituciones democráticas de seguridad, ha resultado en la creación de un aparato novedoso para realizar las actividades de la función de inteligencia. En este caso, la integración de la función de inteligencia con *Smart Power* demanda la invención de un distinto tipo de “organización de información” junto con novedosos procedimientos operativos, para reemplazar la versión tradicional de inteligencia que se basa en apreciaciones sobre “amenazas”.

Los servicios de inteligencia, como cualquier organización burocrática, están interesados en el instinto de su propia conservación (y crecimiento). El camino más directo a la preservación será típicamente para estos servicios demostrar que ellos tienen un producto valioso, y que pueden encargarse a diario de importantes tareas de seguridad. No sólo eso, pero también necesitan demostrarle al público, así como también a los supervisores del gobierno y cuerpos de control, que ellos y sus productos son mejores que los de sus potenciales competidores en las respectivas sociedades, en anticipar y satisfacer las necesidades de los usuarios oficiales de información e inteligencia en asuntos de seguridad interna y externa. Ahora, porque los competidores sí existen en la forma de medios de comunicación masiva, académicos profesionales, centros



de investigación pública y privada, y efectivamente cualquier otro grupo que tenga acceso conveniente a información pertinente que pueda ser verificada, los servicios de inteligencia estarán obligados a demostrar su disposición para comprender y aplicadamente enfocarse en nuevas amenazas y oportunidades.

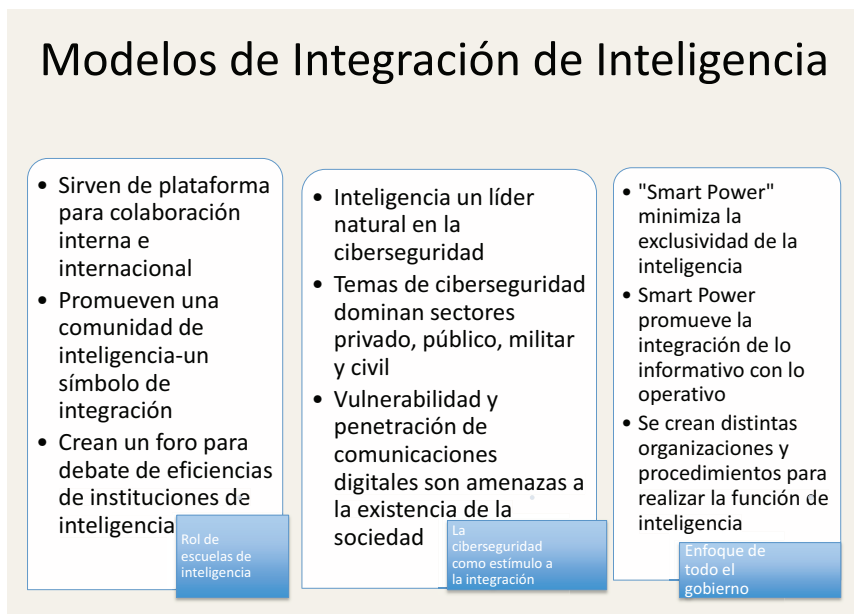


Figura 4. Fuente: Desarrollada por el autor.

Para mantenerse relevante y confiable, todos los servicios de inteligencia se enfrentan al desafío de identificar y emplear personal bien educado y confiable; además, de proveer al personal un futuro profesional estable, con entrenamiento técnico y desarrollo de conocimientos profundos sobre una gama de objetivos o blancos potenciales de los servicios, y luego ofreciéndole una educación continua mediante programas de desarrollo profesional de clase mundial.

Los posgrados en inteligencia y un énfasis en el rol de la inteligencia en el tema de ciber seguridad sirven para invitar a personas particulares y a las instituciones de seguridad a insertarse en el proceso de plena integración del ciudadano junto con la del Estado. En el ambiente militar contemporáneo,

## Gestión de Inteligencia en las Américas

donde los oficiales de países avanzados se encuentran obligados a inventar un proceso creíble para el asesoramiento a oficiales de alto rango del país anfitrión, sobre el diseño y formación de instituciones nacionales responsables de la seguridad, encontramos la demanda para cumplir de modo innovador con la tarea de recolectar información y lograr su perfección como inteligencia para sustentar la toma de decisiones a nivel nacional.

En estos ambientes bilateral y multilateral, la recolección y perfeccionamiento de información no siempre puede llamarse un proceso de “inteligencia” debido a las sensibilidades locales e internacionales al respecto, y de acuerdo con restricciones legales a esta actividad sumamente política. De todos modos, considerados como elementos de la función burocrática, las interacciones personales en el contexto de recoger y procesar información útil para propósitos de seguridad nacional, cuenta con los mismos medios y fines que tiene el fenómeno de inteligencia nacional o estratégica, como la elaborada en cualquier sociedad. Por eso, una conceptualización más comprehensiva que antes de la función de inteligencia, creada para cumplir con las demandas evolucionadas de la seguridad internacional, se está concretando en términos prácticos vía una aproximación fundamental a la gestión de información, sin el típico refugio del secreto.

### Plan del libro

Los cuatro ámbitos burocráticos estatales de gestión de inteligencia son el tema de los ensayos que se presentan a continuación en cuatro secciones. Los comentarios que dan inicio a cada sección revisan los trabajos respectivos, y corresponden a la reflexión de un observador bien experimentado en el tema desde una perspectiva académica y/o profesional, la cual no compete a las instituciones en las cuales se desempeñan.



**Sección I**  
**Fiscalización de Inteligencia en el Contexto**  
**Democrático:**  
**Dimensiones Éticas y Legales**



### Revisão da Primeira Secção

Marco Cepik

Os ensaios que compõe a primeira parte do livro *Gestión de Inteligencia en las Américas* tratam da legitimidade dos sistemas nacionais de inteligência, em especial do aparato legal que regula, controla e fiscaliza a atividade de inteligência. Os textos também examinam o contexto filosófico da inteligência, contribuindo para o desenvolvimento de um *ethos* profissional nos serviços governamentais de Inteligência.

O capítulo de Andrés Gómez de la Torre Rotta e Arturo Medrano Carmona analisa o modo pelo qual o contexto legal contribuiu para a evolução do sistema de inteligência do Peru, com uma breve mirada em outras experiências na região. O ensaio é notável por sua consideração com a evidência empírica. De importância particular é a análise dos desenvolvimentos legais recentes no Peru (Lei 29915/2012 e Decreto Legislativo 1141/2012), voltados para o fortalecimento das conexões entre segurança, defesa e inteligência, bem como para a definição do papel da *Dirección Nacional de Inteligencia* (DINI).

Em seguida, Joanisval Brito Gonçalves traz uma revisão consistente dos vários tipos de controle da atividade de inteligência, no Brasil e em outros países, especialmente o Canadá. Ao mesmo tempo, a opinião do autor sobre a Lei de Acesso à Informação no Brasil (Lei nº 12.527/2011), embora explicitamente proferida como opinião doutrinária e de princípio, é sintomática da falta, no Brasil, de pesquisas empírica e teoricamente fundamentadas sobre os desafios do segredo governamental e do direito à informação, nos termos realizados ao longo dos últimos vinte anos nos Estados Unidos.

Carlos Maldonado Prieto, autor do terceiro artigo, aborda o tema da ética na atividade de inteligência, construindo um *framework* analítico apropriado para o assunto. Ele oferece opiniões aguçadas e percepções informadas pela observação atenta dos desenvolvimentos institucionais na América Latina e Europa do Leste. Vale esperar que este ou outros autores aprofundem a reflexão sobre o nexos entre Inteligência e Direito Público Internacional, mencionado brevemente no texto. Afinal, tal nexos embasa a discussão de um conjunto potencialmente universal de normas éticas para a atividade internacional de inteligência. Em particular, a questão dos assassinatos políticos

poderia ser melhor enquadrada como parte do problema teórico mais amplo acerca da relação entre ações encobertas e a área governamental responsável pela inteligência. Ainda assim, há que se concordar com o autor em relação à relevância ética de se tratar os serviços de inteligência como um serviço público no mundo contemporâneo.

Finalmente, o último artigo desta seção, intitulado *Derechos Humanos y Ética de La Inteligencia: Análise de Casos Cinematográficos, de autoria* de Moira Nakousi Salas e Daniel Soto Muñoz, debate o dilema dos imperativos da atividade de inteligência em uma democracia, onde a necessidade de prevenir ou reprimir uma ameaça está em conflito com os custos sociais da restrição da liberdade e dos direitos individuais. Como os autores apontam, a indústria cinematográfica tem fornecido exemplos úteis a respeito de tais custos nas ditaduras. Da violação do direito à intimidade praticada pela polícia política da Alemanha Oriental no filme *A Vida dos Outros* (Das Leben der Anderen), de Florian Henckel von Donnersmarck (2006), até a impunidade de um criminoso comum que trabalhava para uma agência de segurança durante os anos da ditadura militar, no filme argentino *O Segredo dos teus Olhos* (El secreto de sus ojos) de Juan José Campanella (2009), mas principalmente através do exame detalhado do filme *Unthinkable* de Gregor Jordan (2009), os autores enfatizam a necessidade de ajustar métodos de inteligência e contra-inteligência para uma moldura judicial e ética com a finalidade de garantir o respeito aos direitos humanos.

Juntos, os quatro capítulos da primeira seção constroem de maneira provocativa uma posição firme a respeito dos aspectos legais, éticos e políticos envolvidos no gerenciamento da inteligência nas Américas.

**Marco Cepik** é Professor Associado na Universidade Federal do Rio Grande do Sul (UFRGS, Brasil - <http://lattes.cnpq.br/3923697331385475>), também Diretor do Centro de Estudos Internacionais sobre Governo (CEGOV - <http://www.cegov.ufrgs.br>). Contacto: [marco.cepik@ufrgs.br](mailto:marco.cepik@ufrgs.br).

## Leyes de Inteligencia en el Perú y Latinoamérica: Evolucion Histórica, Jurídica e Institucional

Andrés Gómez de la Torre Rotta  
con el apoyo de  
Arturo Medrano Carmona

*El tercer artículo [de Luis Iberico], alumbra el compromiso comunitario de una sociedad que toma las riendas de su destino, decide refundar al propio Estado y sus servicios.*<sup>62</sup>

—Fernando Cocho Pérez

### Introducción

El 27 de enero del 2012, la inteligencia del Estado civil peruana hubiera cumplido 52 años, desde el inicio del primer Servicio de Inteligencia del Estado (SIN), órgano rector a nivel político-estratégico. No obstante, el 14 de septiembre del 2000, fuimos testigos de la caída del mismo servicio, en excreables circunstancias de sub-empleo o empleo típico de agencias de inteligencia para fines político-partidario personales.

El propósito del presente trabajo es revisar -en el caso del Perú- la historia de cuáles fueron los orígenes de la inteligencia civil, cómo evolucionaron las leyes y las falencias de las mismas en materia de inteligencia, así como los avances legales en materia de inteligencia de Panamá, Colombia, Ecuador, Uruguay, Venezuela y Bolivia.

Así mismo, se busca identificar los caminos hacia los controles democráticos (fiscalización y control) en materia de inteligencia que los países anteriormente citados han seguido. Entre dichos controles tenemos los mecanismos de controles externos, los cuales subclasificamos en controles parlamentarios,<sup>63</sup> judiciales,<sup>64</sup> y económico-financieros.<sup>65</sup>

Al respecto, debido a la evolución de las leyes surge una interrogante: ¿en un Estado de Leyes, cuál es el estado legal en Latinoamérica en materia de control de inteligencia, en términos de tendencias centralizadoras (que dan una autonomía o auto-control al poder ejecutivo y sus órganos de inteligencia),



y tendencias descentralizadoras (que ceden un rol más amplio a los controles externos -poderes legislativos y judiciales- también autónomos)?

Tal como dice Diego Navarro Bonilla, “la actividad de Inteligencia se sustenta históricamente en el concepto de secreto”;<sup>66</sup> sin embargo, lo que se busca es conocer las mejoras en materia de inteligencia dentro de contextos democráticos, las mismas que van desde la formación académica adecuada hasta los controles democráticos.

### Orígenes de la inteligencia en el Perú

Los orígenes históricos de la inteligencia en el Perú se remontan a la creación de dependencias de inteligencia militar, dentro de las fuerzas armadas. A fines de los años cincuenta los militares crearon la escuela y el servicio de inteligencia en el ejército, y formarían a cuadros de inteligencia en su institución posteriores que marcarían una época y etapa. El ejército asimiló entre otros aspectos los afrancesados conceptos de *seguridad, desarrollo y pacificación*, debidos a su filiación francófila, con visión contra-subversiva francesa, particularmente con la experiencia de la guerra de Argelia.<sup>67</sup>

El establecimiento de un organismo de inteligencia de alcance nacional en el nivel político estratégico se hace realidad, como corolario de los años cincuenta en una década plena de modernización institucional del Ejército peruano, y por intermedio de un Decreto Supremo sin número, cuando el 27 de enero de 1960 se creó el (nominalmente civil) Servicio de Inteligencia Nacional (SIN).

Posteriormente, otro Decreto Supremo complementario emitido el 30 de septiembre del mismo año, estableció pautas adicionales, desde la perspectiva de institucionalizar la relación del SIN dentro del aparato estatal y de los órganos incorporados e integrantes. En ese sentido, el Decreto Supremo del 30 de septiembre de 1960, de tres escuetos artículos, señalaba en su tercer considerando la necesidad de desarrollar la relación del SIN con los Ministerios de Estado.<sup>68</sup> El empleo de los Decretos Supremos,<sup>69</sup> como jerarquía normativa para regular inteligencia, deben entenderse en la línea de la doctrina jurídica peruana; al respecto, Víctor García Toma señala claramente el derrotero: “Se trata de preceptos de carácter general que regulan la actividad sectorial y multisectorial a nivel nacional. Se encargan de normar

## Gestión de Inteligencia en las Américas

y supervigilar la organización y funcionamiento de los servicios públicos nacionales o las actividades de dichas instituciones (...).<sup>70</sup> Consideramos fundamental, en la línea de García Toma, el carácter de *servicio público* a la actividad de inteligencia del Estado y es así que en el año 1960 nace el nombre del organismo: “Servicio”.

El SIN peruano se entiende en las lógicas de Guerra Fría de los nuevos servicios de inteligencia latinoamericanos de contención al comunismo y lucha contra-subversiva; cuya nomenclatura nos resulta ser bastante conocida: la CIDE y el SFICI argentino y brasileño respectivamente (1946), el DFS mexicano (1947) y el SIC-DAS colombiano (1953). Luego seguiría Venezuela, en 1969, con fuerte apoyo de los Estados Unidos y sus respectivas agencias en la creación de la DISIP, durante el gobierno democrático del Presidente Rafael Caldera (COPEI).<sup>71</sup>

Pero ninguno de estos Decretos Supremos peruanos de inteligencia, del año 1960 consideraron la existencia o puesta en marcha de controles públicos sobre la actividad de inteligencia. Debe señalarse que eran coyunturas embrionarias del desarrollo de las instituciones y actividades de inteligencia, que se construyeron en el Perú, dentro del contexto de triunfo de las revoluciones china (1949) y especialmente cubana (1959), y de la expansión de la técnica de guerra no convencional, irregular, insurgente, revolucionaria o subversiva. Sin embargo, es rescatable la parte considerativa del Decreto Supremo sin número del 27 de enero de 1960:

Que la complejidad del problema que plantea actualmente la Defensa Nacional hace necesario contar con organismos especiales para el mejor cumplimiento de las funciones que la Constitución y las leyes asignan al Presidente de la República.

Aquí encontramos un importante coto o freno al desarrollo de la actividad de inteligencia del Estado: ésta se subordina, como ente productor, a un *consumidor privilegiado* o *tomador de decisiones* que ejerce *de jure* funciones establecidas por la constitución y las leyes.

## Evolución y distorsiones de la legislación de inteligencia en el Perú entre 1960 y 1970

Durante la Guerra Fría el SIN comienza a ser empleado en el Perú para operaciones políticas a mediados de los años sesenta, curiosamente en democracia, bajo el primer gobierno del partido Acción Popular del entonces Presidente Fernando Belaúnde, colaborando con el Ministerio de Gobierno y Policía con la requisita de libros y textos de origen marxista, en el contexto de la aparición de guerrillas pro-castristas en territorio peruano (1965), promovidas por el modelo insurreccional exportado por Cuba, las que serían reprimidas con alto protagonismo de la inteligencia del ejército. Sin embargo, la predominancia de la inteligencia militar (especialmente del ejército y marina de guerra) se percibe claramente en el Golpe de Estado militar del 3 de octubre de 1968, donde la inteligencia del ejército actuaría como eje central, mientras que el SIN nada supo de ello, pues sus jefes no fueron consultados para la perpetración del mismo.

Ante el Golpe de Estado la reacción de los jefes del SIN fue paradójica: su Jefe, el General Carlos Linares Molfino renunció por su cercanía con el depuesto Presidente constitucional Fernando Belaúnde, mientras que su Sub-Jefe, el Coronel Eduardo Segura Gutiérrez se plegó al *putsch* militar, convirtiéndose posteriormente en el Jefe del SIN.

El 25 de marzo de 1969 el autodenominado Gobierno Revolucionario de las Fuerzas Armadas (GRFA) del Presidente de facto, General Juan Velasco emite la Ley Orgánica de la Presidencia de la República, Decreto Ley N° 17532, que en su artículo 2° coloca al SIN en relación de dependencia directa de la Presidencia de la República.

Finalmente, el Decreto Ley N° 19351, perfecciona el Decreto Supremo del 30 de septiembre de 1960, en cuanto a la articulación de relaciones y de coordinación entre los integrantes del Sistema de Inteligencia Nacional (SINA). No existe alusión alguna en esos dispositivos referente a aspectos relacionados con rendición de cuentas, controles democráticos, supervisión o fiscalización.

Un Capitán de Navío de la Marina de Guerra del Perú publica un importante trabajo en el año 1973, en la *Revista de Marina*: “¿Qué es un Servicio de Inteligencia?”<sup>72</sup> Él aborda en el citado artículo diversos ángulos de la actividad,

## Gestión de Inteligencia en las Américas

problemática, tareas y composición de los servicios de inteligencia, siendo probablemente el primer aporte en su género en el país, donde hasta entonces habían primado estudios y publicaciones sobre criptografía.

Finalmente, sobre los Decretos Leyes promulgados en esta etapa, la doctrina jurídica y constitucional señala claramente su vinculación a los regímenes *de facto*, como fue el clarísimo caso del GRFA (1968-1980), teniendo el Decreto Ley N° 19351 de 1972 lo que en doctrina jurídica se conoce como *la teoría de la continuidad*, puesto que no habría sido considerado dentro de la caducidad con la vuelta a la democracia el 28 de julio de 1980 y habría tenido vigencia hasta el 10 de febrero de 1984, cuando es derogado en virtud del artículo 29° del Decreto Legislativo N° 270.

### La guerra contra el terrorismo: 1980-1990

En 1980, el Partido Comunista Peruano – Sendero Luminoso (PCP-SL) planteó una guerra revolucionaria no convencional contra el Estado peruano. Empleando diversas modalidades delictivas, el PCP-SL obligó una profunda revisión de los esquemas de contrainsurgencia, entre ellos del Sistema de Inteligencia Nacional (SINA).

Para tales efectos, la Ley N° 23720<sup>73</sup> otorgó al poder ejecutivo facultades delegadas para legislar sobre inteligencia, y como resultado de la inconveniente abdicación y decline congresal, y dada la celeridad en mejorar la estructura y normas de inteligencia nacional, son elaborados los Decretos N° 270 y N° 271 a través de los denominados procedimientos de legislación delegada. El primero sobre el SINA, y el segundo referente al Servicio de Inteligencia Nacional (SIN). Estos dispositivos fueron diseñados en la intensidad de una cruenta y nefasta guerra subversiva, y en la conducción y jefatura, por primera vez en la historia del SIN, de autoridades navales. Estimulante fue el establecimiento mediante dichas normas de un Consejo Superior de Inteligencia (CSI) que intentó articular la inteligencia en democracia, ya que la idea original venía de la legislación generada por el gobierno militar, de un Decreto Ley del año 1972.

Gustavo Gorriti Ellenboghén, destacado periodista peruano, escritor y formador de opinión, en su libro sobre Sendero Luminoso,<sup>74</sup> dedica capítulo completo sobre la trama de la inteligencia peruana en la década de los ochenta,

al que denomina como *Coloquio de Ciegos. La guerra de la Inteligencia*, y en donde analiza de forma descarnada y detallada acerca de las precariedades y falencias institucionales del SINA y del SIN, en el contexto de la lucha contra el terrorismo, con énfasis en el desempeño de la inteligencia policial y del Ministerio del Interior. Gorriti calificó al período del SIN de la década de los años ochenta como *años vegetativos*, y fustiga duramente a su estructura burocrática. Durante el período del primer gobierno de Alan García (1985-1990) son designados dos Jefes del Ejército para el SIN, con lo que se continuaba la línea militarizada en asuntos de inteligencia.

### La policía política o *stasi* andina, y el Estado depredador: 1991 – 2000

Con objeto de reorientar la actividad de inteligencia, el gobierno de Alberto Fujimori propone una drástica reconversión del Sistema de Inteligencia Nacional en el año 1991. Allí aparece la más controvertida ley peruana elaborada en materia de inteligencia: el Decreto Legislativo N° 746, la misma que habría sido diseñada desde las oficinas de Asesoría Jurídica del propio SIN (OTAJ-SIN) a inicios de los años noventa, y en donde hubo participación de antiguos trabajadores del SIN que provenían de la década de los sesenta y ochenta.

La filosofía del Decreto Legislativo N° 746 se encuadraba en los términos de perfilar una dependencia de inteligencia peruana, de rasgos muy similares a la de los servicios de inteligencia de Europa Oriental de la época de Guerra Fría, a lo que frecuentemente hemos denominado como una “*Stasi* andina”.<sup>75</sup>

Quienes justificaron el esquema legal de inteligencia entre 1991 y 1992 vendieron su producto como un modelo “exitoso” basado en el “centralismo unificado de mando”, también llamado “modelo de dirección central”, o “centralista unificado”, que tendía a evitar la supuesta dispersión interagencial al interior del SINA, heredada de 1984. Asombrosamente pero con bastante anterioridad, al igual que el SIN peruano de los años noventa: “Al contrario que los servicios secretos de los países democráticos, la Stasi era el puntal del poder del Estado”.<sup>76</sup> El abogado Luis Piscocoya Salinas en su condición de analista del frente interno (DINFI) de la Dirección Nacional de Inteligencia Estratégica (DINIE –Centro Nacional de Inteligencia– CNI), ha sido uno de los escasos interesados en hurgar sobre el modelo centralista de inteligencia peruano.<sup>77</sup>

Piscocoya ha sido especialmente crítico del CNI (2001 – 2006).

## Gestión de Inteligencia en las Américas

Para dichos efectos el Consejo Superior de Inteligencia (CSI) -ente de coordinación interagencial y modelo colegiado de toma de decisiones- fue eliminado de las normas legales de 1991 y 1992. El SIN hasta entonces, sin el CSI “que-todo-lo-puede”, controlaba todo en inteligencia, como la SAVAK del Shá de Persia, y los Partidos Comunistas orientales, con sus respectivas policías políticas; el SIN estaba en todas partes.<sup>78</sup> Las capturas de mandos terroristas efectuadas en los años 1992, 1993 y 1994, debido a una coyuntura de múltiples factores, contribuyeron a fortalecer el espejismo de un modelo centralista de inteligencia “exitoso” que marcaba distancias con los supuestos “errores” cometidos en los años ochenta bajo un régimen de inteligencia más reglamentado; adicionalmente, ello resulta ser un cuestionamiento a las administraciones militares de inteligencia de esa época, entre ellos los jefes del SIN.

En el período de los años noventa, el SIN contribuiría decisivamente a la generación y construcción en el Perú de un típico *Estado depredador*.<sup>79</sup> Una prueba irrefutable de la asombrosa similitud del Decreto Legislativo N° 746 del 11 de diciembre de 1991, con la filosofía y modelo de servicio y acción de inteligencia perfilado en la Europa oriental comunista de Guerra Fría, fue el artículo 21° de la citada norma.<sup>80</sup>

Luego vendría el Decreto Ley N° 25635 de 1992 posterior al autogolpe civil fujimorista. Se trata de una norma bastante parecida a la promulgada en 1991, salvo por algunos cambios *cosméticos*.<sup>81</sup>

### El derrumbe del SIN

El SIN de los años noventa fue puesto en evidencia -entre otros- por el congresista Luis Iberico, al poner en conocimiento de la ciudadanía el video Kouri - Montesinos, extraído de las entrañas del SIN, y difundido el 14 de septiembre del 2000. Tal fue el impacto de ese suceso que tras el vergonzoso derrumbe del SIN cayó un régimen político autoritario, que se sustentó justamente en los servicios de inteligencia como eje de su acción de gobierno.<sup>82</sup>

Alberto Fujimori cayó con su servicio de inteligencia, del que al parecer nunca pudo controlar ni afirmar su propia autoridad política, y a la que él contribuyó decisivamente a fortalecerla, reconvirtiéndola nocivamente entre 1991 y 1992. No olvidemos que Fujimori, en cierta oportunidad, calificaría al SIN como el mejor servicio de inteligencia del mundo.

Alberto Bolívar Ocampo, quien desempeñó funciones en el SIN de los noventa -como el suscrito- describe lo que fue el SIN de la década de los noventa:

Entre 1990 y 2000, Alberto Fujimori y Vladimiro Montesinos convirtieron a la estructura de Inteligencia peruana en una muy eficiente maquinaria de espionaje político al interior del país, de control de medios de comunicación y de sujeción de voluntades individuales y colectivas, desnaturalizándose totalmente el trabajo de inteligencia (...) las fuerzas armadas y la policía nacional se convirtieron en la mayor amenaza a la seguridad nacional del Perú [en referencia a la situación de la década de los noventa] (...) internamente se dedicaba a labores ajenas a sus verdaderas funciones (...) [en relación a la Inteligencia peruana del segundo quinquenio, en los años noventa].<sup>83</sup>

El SIN es desactivado por el propio gobierno de Alberto Fujimori, el mismo que contribuyó decisivamente, en la década de los noventa, a “potenciarlo”. Lo hizo mediante un Proyecto de Ley del Poder Ejecutivo (PL N° 461–2000/CR) convertido luego en Ley de Desactivación del Servicio de Inteligencia Nacional, Ley ordinaria N° 27351, en el mes de octubre del año 2000 (en su sexto artículo derogó expresamente el Decreto Ley N° 25635 de 1992). Previamente, en un último intento del gobierno fujimorista por mantener el control de inteligencia, durante el mes de agosto del año 2000, en el contexto de la instalada mesa de diálogo de la OEA entre el gobierno y la oposición, el poder ejecutivo presentó una inédita proposición legislativa: el Proyecto de Ley N° 258–2000/CR para la creación de una *Central Nacional de Inteligencia*, a la que erróneamente se le quiso dotar y dar rango de ley orgánica,<sup>84</sup> y que entre otros aspectos consideraba la creación de una *Junta Consultiva de Inteligencia* (JCI) como ente de coordinación interagencial entre los organismos componentes del SINA. La citada *Junta Consultiva de Inteligencia*, intentaba reeditar una suerte de “nuevo” Consejo Superior de Inteligencia, del esquema normativo de 1984. Lamentable y patética fue la extensión terminal del SIN con el empleo de Decretos de Urgencia (D.U. N° 018 y D.U. N° 046, respectivamente, de febrero y abril del 2001) para permitir la continuidad de la producción de inteligencia.

## Gestión de Inteligencia en las Américas

### Aparecen las mejoras: 2000-2012

Ciertamente en la década 2000-2010 hubo errores. Estos se notan especialmente en los intentos por reconstruir nuestro sistema de inteligencia,<sup>85</sup> pese a existir jefes de inteligencia preparados, probos, honestos, conocedores y solventes en estos tres últimos gobiernos consecutivos: de transición (2000-2001), de Perú Posible (2001-2006) y del APRA (2006-2011).

Sobre el particular, la Defensoría del Pueblo del Perú,<sup>86</sup> había tomado conveniente nota de lo acontecido en el trájín de la inteligencia peruana de los noventa,<sup>87</sup> destinado a formular propuestas para contribuir al diseño de un servicio de inteligencia que cuente con los controles democráticos necesarios para evitar la comisión de excesos que afecten los derechos de las personas. Dicho documento fue elaborado por la Defensoría Especializada en Asuntos Constitucionales, cuya versión preliminar fue entregada a los miembros del grupo de trabajo sobre inteligencia, facilitado por la Organización de Estados Americanos en Lima. El estudio propuso insertar algunos artículos a una futura ley de inteligencia. En las conclusiones del documento señaló que una Comisión del Congreso de la República sea la encargada de dedicarse únicamente al tema objeto de la cuestión, dejando claro que la Comisión de Defensa Nacional, Orden Interno, no era la idónea para sumir el encargo.

De esta manera incidió en diseñar adecuadamente algunos procedimientos no previstos en las Leyes de Inteligencia de 1991 y 1992, eso es en la aprobación, verificación y cumplimiento de lo que en su momento denominó como “Planes Operativos Anuales”, lo que luego sería conocido como “Plan Anual de Inteligencia” (PAI). También abordó el tema de la transparencia, el secreto<sup>88</sup> y secrecía<sup>89</sup> de Estado, el principio de publicidad, la información clasificada y su manejo, lo que es consecuente con la promulgación en 2002 de una Ley de Transparencia y Acceso a la Información Pública.

En el contexto de la inteligencia peruana post-Montesinos, se entiende la Ley ordinaria N° 27479 promulgada por el Congreso, en el mes de junio de 2001, aprobada sobre la base de cinco Proyectos de Ley previos durante el gobierno de transición del entonces Presidente Valentín Paniagua Corazao (Acción Popular), que creó el Consejo Nacional de Inteligencia (CNI) y la Dirección Nacional de Inteligencia Estratégica (DINIE). Fue la primera vez



que la inteligencia peruana era regulada por una Ley Ordinaria promulgada por el Congreso de la República.

La grave y gran sorpresa de la nueva legislación de inteligencia promulgada, fue la asombrosa similitud con la letra y espíritu de su antecesora, el Decreto Ley N° 25635 de 1992. El calco fue tan nocivo como peligrosamente descarado.<sup>90</sup>

En ese sentido, en el Perú se produjo una situación tan paradójica como inusual, y en extremo grave. La misión de la Universidad de Harvard, *Justice in Times of Transition*, fue convocada en Lima por el Jefe del CNI, el destacado periodista Juan Velit, durante el año 2002 para emitir un Informe de su Grupo de Trabajo internacional denominado como: *Recomendaciones para la reforma de la Inteligencia en el Perú a la luz de la experiencia de otros países del mundo*. El proyecto convocó a destacados expertos internacionales en el tema, para estudiar las fortalezas y vulnerabilidades de la legislación sobre inteligencia generada en democracia. Nos detenemos en dos de los expertos convocados: José Manuel Ugarte de Argentina<sup>91</sup> y Manolo Vela de Guatemala. Ambos señalaron en los estudios respectivos elaborados para el grupo de tareas de Harvard, lo poco conveniente que era copiar artículos cuasi textuales provenientes del Decreto Ley N° 25635 de 1992 en la Ley N° 27479 del 2001, especialmente en el sensible tema operativo de la actuación de inteligencia.

No era la única señal que aparecía en el año 2001, una vez recuperada la democracia, parafraseando al mexicano Raúl Benítez Manaut, también del Grupo Harvard, como propia de un “Estado autoritario”. El artículo 9° de la entonces vigente Ley N° 27479, que señalaba textualmente: “El Sector Público y Privado proporciona al Sistema de Inteligencia Nacional la información que es necesaria para la Seguridad y el Desarrollo Nacional”, no aclaraba los procedimientos de envío de la información generada del sector público y privado al SINA, supuestamente necesaria para garantizar la “seguridad nacional”. En ese artículo asomaba amenazadora presencia, el Decreto Legislativo N° 746 de 1991 y especialmente su tenebroso y anteriormente citado artículo 21°, acorde al patrón clásico y estilo de obtención o colección de información de las más recalcitrantes policías políticas comunistas de la Europa Oriental de Guerra Fría, como la *Stasi* germano-oriental, la *Securitate* rumana del dictador Nicolae Ceaucescu, o la NKVD (precursora de la KGB) de Yosif Stalin en la ex URSS.

## Gestión de Inteligencia en las Américas

Prueba de la escasa voluntad política, preocupación y especialmente desidia de algunas de las nuevas autoridades sobre el sector inteligencia, es el hecho incontrovertible que la Ley N° 27479 del 2001 nunca tuvo Reglamento. Ya en democracia, en el sector inteligencia hubo insistencia de alguna voz oficialista, que para tal Reglamento de la nueva ley recayera la clasificación de Secreto.

La Ley N° 27479 incursionó tibia, pero novedosamente -en su artículo 36°, y en la Quinta Disposición Transitoria- en el tema de la fiscalización parlamentaria sobre inteligencia.<sup>92</sup> Se incidió exclusivamente en el tema de la ejecución presupuestal.

Desde el año 2002 ya existían y se acumulaban progresivamente diversos Proyectos de Ley para modificar y perfeccionar la Ley N° 27479; la disposición de los legisladores de ese momento era evidente. Había que perfeccionar y reorientar esa norma. En el año 2003, se percibió el interés del gobierno de turno para diseñar un nuevo marco normativo de la inteligencia nacional. Dichos Proyectos de Ley, se encontraban en la Comisión de Defensa Nacional, Orden Interno, Inteligencia, Desarrollo Alternativo y Lucha contra las Drogas del Congreso de la República, listos para ser examinados y luego acumulados con miras a la elaboración de un pre dictamen<sup>93</sup> respectivo, que supusiera el ingresarlos a la agenda del debate en la Comisión Parlamentaria, con miras a la elaboración de una nueva ley de inteligencia del Estado.

Por otro lado, el Ministerio de Justicia encaró el tema de inteligencia con un sugestivo y encomiable aporte.<sup>94</sup> Dicho documento desarrolló minuciosamente el control judicial sobre operaciones de inteligencia. También, una Comisión Especial constituida por el poder ejecutivo, en virtud de la Resolución Suprema N° 097-2004-PCM,<sup>95</sup> emitió su propio documento<sup>96</sup> donde desarrollaba el tema de los controles democráticos, la legitimación, la transparencia y rendición de cuentas. Adicionalmente, la citada Comisión elaboró una minuta o borrador de Proyecto de Ley, para la creación de una Agencia de Inteligencia Estratégica (AIE), que posteriormente el poder ejecutivo hizo suya. El citado borrador o minuta del Proyecto de Ley original de la AIE consideró convenientemente la existencia de principios reguladores de la actividad de inteligencia (artículo 4° del documento), y también de la conformación de una Comisión independiente de inteligencia en el Congreso, pero dicho proyecto nunca se convirtió en Ley.<sup>97</sup>

En el año 2005, fue promulgada por el Congreso la Ley ordinaria N° 28478, *Ley del Sistema de Seguridad y Defensa Nacional*, por la cual se inserta al Sistema de Inteligencia Nacional (SINA), como componente o sub-sistema del Sistema de Seguridad y Defensa Nacional (art 4º, b). El capítulo III de la norma, en su artículo 14º señala textualmente que: “El Sistema de Inteligencia Nacional forma parte del Sistema de Seguridad y Defensa Nacional y se estructura para producir inteligencia y realizar actividades de contrainteligencia necesarias para la Seguridad Nacional. Se rige por su propia ley y reglamento.”

Finalmente, luego de 14 Proyectos de Ley previos sobre el asunto, de acumular, pre-dictaminar, dictaminar, aprobar en el pleno, levantar las observaciones del Ejecutivo por la vía del mecanismo de insistencias y allanamientos, por la entonces Comisión de Defensa Nacional, Orden Interno, Inteligencia, Desarrollo Alternativo y Lucha contra las Drogas, en el mes de enero del año 2006, es promulgada por el Congreso la Ley del Sistema de Inteligencia Nacional -SINA y de la Dirección Nacional de Inteligencia- DINI, Ley Ordinaria N° 28664.<sup>98</sup>

La citada nueva Ley peruana del 2006 trae varias novedades, por ejemplo: por primera vez en la historia normativa peruana sobre la materia, el mecanismo de control judicial recayó sobre las denominadas “Operaciones Especiales”,<sup>99</sup> definición a través del cual se evitó en todo momento insertar el de operaciones “intrusivas”, “clandestinas”, “invasivas” o “encubiertas”. Así también, el Capítulo III, titulado “Control de la Actividad de Inteligencia”, señala minuciosamente en su artículo 20º el mecanismo de control judicial para la ejecución de las operaciones especiales:

- Para el control judicial de las operaciones especiales, la Corte Suprema de Justicia de la República designa dos Vocales Superiores Ad hoc.
- Las operaciones requieren autorización judicial otorgada por cualquiera de los dos Vocales Superiores Ad hoc del Poder Judicial... Todo el proceso constituye información clasificada como secreta.
- Las operaciones especiales son solicitadas debidamente por el Director Ejecutivo de la Dirección Nacional de Inteligencia – DINI a cualquiera de los dos Vocales Superiores Ad hoc del Poder Judicial.

## Gestión de Inteligencia en las Américas

- En caso de peligro de la seguridad nacional y por la urgencia de las circunstancias es necesario realizar una operación especial, el Director Ejecutivo de la Dirección Nacional de Inteligencia – DINI, puede excepcionalmente autorizarla con cargo a formalizar la solicitud de inmediato ante el Vocal Superior Ad hoc, quien en el plazo de veinticuatro horas puede convalidar o disponer la inmediata paralización de la operación especial (...).
- Las resoluciones del Vocal Superior Ad hoc autorizando operaciones especiales tienen carácter vinculante para todas las entidades públicas y privadas que deben coadyuvar a su realización, debiendo observar las disposiciones sobre información clasificada (...).
- La solicitud motivada del Director Ejecutivo de la Dirección Nacional de Inteligencia – DINI y la resolución que emite el Vocal Superior Ad hoc, se tramitan dentro de las veinticuatro horas de presentada; en forma personal e indelegable.
- Ante resolución denegatoria del Vocal Superior Ad hoc, procede recurso de apelación ante la Sala que integra; la apelación se tramita y resuelve en el plazo de veinticuatro horas.

En la Ley N° 28664, es destacable que las resoluciones del Vocal Superior Ad hoc en las que autorizan operaciones especiales que tienen carácter vinculante, son excluyentes para la Unidad de Inteligencia Financiera del Perú (UIF-PERÚ) en tanto contravenga su autonomía funcional, técnica y administrativa.<sup>100</sup> La UIF-PERÚ está facultada para solicitar, recibir y analizar información a través de los Reportes de Operaciones Sospechosas (ROS).<sup>101</sup>

En materia de fiscalización parlamentaria, es creada una Comisión Ordinaria de Inteligencia, que se independiza de la de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha contra las Drogas, tal como lo era tradicionalmente. La Ley N° 28664 en su artículo 21° señala las atribuciones de la Comisión de Inteligencia, las que no pueden entenderse sin una estricta concordancia con el Reglamento del Congreso. El artículo 22°, regula la composición de la Comisión de Inteligencia; entre 5 o 7 miembros permanentes o titulares elegidos por el Pleno del Congreso por todo el período parlamentario, sin miembros accesorios<sup>102</sup> en estricta concordancia con los

principios de pluralidad y especialidad. Las sesiones de la Comisión son de carácter secreto, sólo cuando las circunstancias así lo ameriten.

La primera prueba de fuego de la citada Ley ocurrió durante dos crisis generadas por la fuga de información de un organismo componente del SINA: la Dirección de Inteligencia Naval (DINTENAV).<sup>103</sup> En los casos *MARTE-DINTEMAR* (2007) y *BTR* (2009) se transgredió la citada ley en cuanto a la obligación de guardar secreto y al manejo de información clasificada<sup>104</sup> debido a las actividades intrusivas que en ese entonces realizaron los organismos privados de inteligencia con personal militar en actividad. En cuanto al caso *BTR*, el personal militar de entonces se encontraba en situación de retiro, y se vulneró el monopolio estatal de obtención de información clasificada.<sup>105</sup>

Ante tales efectos y coyunturas descritas, la Comisión Ordinaria de Inteligencia crea un Grupo de Trabajo<sup>106</sup> presidido por el congresista José Urquiza (Partido Nacionalista), el mismo que emitiría un Informe Final,<sup>107</sup> y que posteriormente sería aprobado por el Pleno del Congreso.

### Falencias en el andar jurídico e institucional de la inteligencia peruana post ley n° 28664 del 2006

En este contexto, bien vale la pena recalcar acerca de los errores de percepción, cometidos por la primera Presidencia de la Comisión Ordinaria de Inteligencia, estrenada desde la primera legislatura del período legislativo 2006-2007. La primera de ellas fue el intentar convertir a la Comisión en *consumidora* o *usuaria* del producto final de inteligencia. Ello se evidenció cuando dicha instancia parlamentaria demandó al Sistema de Inteligencia (SINA) el envío regular de *Notas de Información*, *Notas de Inteligencia*<sup>108</sup> y *Estudios Especiales de Inteligencia*, cuando el poder legislativo no toma decisiones, sólo tiene funciones de fiscalización y legislación en su propio ámbito.

Otro de los errores anteriormente señalados, por parte de esa misma primera Presidencia de la Comisión de Inteligencia, fue la contratación de asesores provenientes de las fuerzas armadas, que si bien aparentan o dicen ser “expertos en inteligencia”, evidencian desconocimiento del derecho, procedimiento y práctica parlamentaria. Un ejemplo de ello es el alambicado Proyecto de Ley N° 2563/2007-CR. En la citada iniciativa legislativa, nos encontramos

## Gestión de Inteligencia en las Américas

con una colección de propuestas contraproducentes, las cuales describiremos a continuación:

- Una fórmula legal incoherente, que propone peligrosamente una difusa “*Dirección Central*” (modificación por adición al artículo 5.2) del SINA por parte del órgano rector de inteligencia (la DINI), como en el año 1992 con las normas legales del SIN de Fujimori y Montesinos, sin establecer en la Exposición de Motivos, o el Glosario, el alcance administrativo y funcional de tal “dirección central”.
- Introducción del término “*Operaciones Encubiertas*” en la propuesta para la modificación por adición al artículo 20.8, no previsto en la letra y espíritu de la vigente Ley N° 28664, y no complementa tal término explicando su naturaleza o alcances, sea en la Exposición de Motivos o en el Glosario; de igual forma sucede con el introducido, y errado concepto de “gastos reservados,” el que parece ser confundido con el de Régimen de Ejecución Especial.
- Una alambicada duplicidad de conceptos respecto a las atribuciones de la Comisión de Inteligencia, planteadas a modo de adiciones al artículo 21.3 de la ley, que revela un desconocimiento de la estricta concordancia de la Ley de Inteligencia con el Reglamento del Congreso, que tiene fuerza de Ley y que establece muy detalladamente los principios y atribuciones del accionar de las Comisiones Ordinarias del Congreso.

Sin embargo, no todo es opacidad en el plano legislativo; la *Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha contra las Drogas*, en condición de Comisión parlamentaria dictaminadora segunda por principio de especialidad, elaboró un Dictamen impecable dotado de rigurosa y solvente técnica jurídica, recaído sobre el Proyecto de Ley 2563, en sesión ordinaria del 8 de junio del 2010, que tiende a corregir las cosas y marcar una clara diferencia en materia de consecuente técnica legislativa. Los dictámenes de ambas Comisiones, esperan el sueño de los justos para ser debatidos en el pleno del Congreso, existiendo un Oficio de la Comisión de Inteligencia, que solicita se priorice en la agenda del pleno.

De esta manera apreciamos que el proceso político que complica la evolución de los organismos de inteligencia está relacionado con la correlación de

fuerzas parlamentarias, políticas y militares, toda vez que ellas permiten llevar a cabo los cambios legales respectivos en aras de mejoras en materia legal de inteligencia.

### Los controles y fiscalización para inteligencia en América Latina y España

El control judicial y la fiscalización parlamentaria en la Ley peruana N° 28664 del 2006 prosigue de la línea y tendencia de la legislación de inteligencia generada por Brasil, Argentina y Chile sobre el particular.<sup>110</sup> Para el año 2006 desde la óptica de la evolución del derecho y legislación de inteligencia, ya nos encontrábamos con un verdadero y estimulante progresión en dicha materia (véase tabla N° 1):

Tabla 1 Evolución de Legislación en Materia de Inteligencia, 1999 – 2005				
PAÍS	LEY	NOMBRE DE AGENCIA		AÑO
BRASIL	Ley 9.883	Sistema Brasileiro de Inteligencia.	SISBIN	1999
ARGENTINA	Ley 25.520	Secretaría de Inteligencia.	SI	2001
ESPAÑA	Leyes Orgánicas N° 2 y N° 11	Centro Nacional de Inteligencia.	CNI	2002
CHILE	Ley 19.974	Agencia Nacional de Inteligencia.	ANI	2004
MÉXICO	Ley de Seguridad Nacional	Centro de Investigación y Seguridad Nacional.	CISEN	2005
GUATEMALA	Decreto Legislativo 71-2005	Dirección General de Inteligencia Civil.	DIGI	2005

Fuente: Leyes de inteligencia de los citados países. Elaboración propia.

Más control, fiscalización, contrapesos y balances políticos, transparencia, rendición de cuentas e involucramiento activo de todos los poderes del Estado sobre la actividad de inteligencia, resulta ser el denominador común de estas importantes normas promulgadas. Así también, no es menos cierto que en

## Gestión de Inteligencia en las Américas

los últimos años con la democracia, la rendición de cuentas y la publicidad de los actos de gobierno, la transparencia de gestión y la apertura se ha ido perfilando y consolidando en el accionar de este peculiar oficio.<sup>111</sup>

### Avances en materia de control público de inteligencia latinoamericana post-ley peruana del 2006

Posteriormente a la Ley peruana de Inteligencia N° 28664 del 2006, en Latinoamérica se viene generando una nueva normatividad sobre la materia, orientada hacia los controles democráticos a través de mecanismos de controles externos: parlamentarios, judiciales y económico-financieros; esta progresión se da con mayor incidencia, desde luego, en el control público sobre la actividad, sistemas y servicios de inteligencia.<sup>112</sup>

#### *Panamá*

El 20 de agosto del 2008 fue promulgado el Decreto Ley N° 9,<sup>113</sup> que reorganizó el Consejo de Seguridad Pública y Defensa Nacional y creó el Servicio Nacional de Inteligencia y Seguridad (SENIS). La norma estableció en su Título V el *Control Legislativo y Judicial* (previo). Si bien esta norma fue derogada, debido a vicios de forma en su promulgación,<sup>114</sup> constituye un aporte importante en el reciente derecho comparado latinoamericano, sobre regulación de servicios de inteligencia, al establecer “control judicial” previo a través de autorización para adoptar medidas que podrían afectar garantías y derechos ciudadanos; además, la resolución judicial que se emita no tendría naturaleza contenciosa, y sus resultados carecerían de valor probatorio en procedimientos judiciales o administrativos.

#### *Colombia*

El 5 de marzo del 2009, fue promulgada la “*Ley N° 1288, por medio del cual se expiden normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de Inteligencia y Contrainteligencia, cumplir con su misión constitucional y legal*”.<sup>115</sup> El Capítulo III de la citada norma desarrolla el tema del “Control y Supervisión”, y específicamente, en materia de control parlamentario, el artículo 13° crea una “(...) Comisión legal parlamentaria de Seguimiento a las actividades de Inteligencia y Contrainteligencia, (...)”.<sup>116</sup> La inexecutable (no ejecutable por vicio de forma debido al proceso en



cómo se tramitó, el mismo que está en proceso) de la Ley 1288, deja sin soporte legal la inteligencia de este país, por lo que sólo dos proyectos de Ley (Proyecto N° 189-2009 y 195-2011) buscan salvar este vacío legal.<sup>117</sup>

A partir de noviembre del 2011, se creó la Dirección Nacional de Inteligencia (DNI), con el fin de llevar a cabo tareas de inteligencia, y no tareas policiales.<sup>118</sup> Además la DNI tendrá un Inspector General que vigilará el cumplimiento de la ley, supervisará la eficacia y eficiencia de las operaciones y vigilará la implementación del sistema de controles.<sup>119</sup>

### *Ecuador*

En este país, el antiguo andamiaje jurídico de la seguridad nacional fue reemplazado: La vieja Ley de Seguridad Nacional de 1979, que establecía la Dirección Nacional de Inteligencia (DNI) la misma que fue derogada. El gobierno de Rafael Correa, con fecha 15 de mayo del 2008, designó una “Comisión para la investigación de los servicios de Inteligencia militares y policiales ecuatorianos”, un informe que no confronta a los civiles con los militares, sino que sólo trata de corregir los efectos del incidente de Angostura<sup>120</sup> debido a que se detectaron elementos preocupantes de que habrían vinculaciones con organismos de inteligencia externos.

En ese sentido se entiende la promulgación del Decreto Ejecutivo N° 1768 del 8 de junio del 2009, que crea la Secretaría Nacional de Inteligencia (SENAIN), y la nueva *Ley de Seguridad Pública y del Estado* (Registro Oficial N° 35, del 28 de septiembre del 2009, Suplemento). Esta última norma crea un procedimiento de autorización judicial para llevar a cabo las denominadas “Operaciones Encubiertas” de obtención de información, así como de un esquema de rendición de cuentas de gestión de la SENAIN y las más altas autoridades de sus entes ejecutores ante la Asamblea Nacional, por intermedio de una Comisión Especializada pertinente.

### *Uruguay*

En el caso uruguayo, el diputado José A. Amy (Partido Colorado), presentó un Proyecto de Ley en el mes de junio del 2010, para la creación de una *Comisión Parlamentaria de Supervisión de los Servicios de Inteligencia*. El artículo 4° del proyecto, introduce *principios*<sup>121</sup> a los que deberán ajustarse las au-

## Gestión de Inteligencia en las Américas

toridades de inteligencia en la recolección y tratamiento de información. La Obligatoriedad de guardar secreto, está señalada en el artículo 5° del proyecto. Finalmente la futura Comisión, en virtud de principios parlamentarios, como los de pluralidad y proporcionalidad, estará integrada por todos los partidos integrantes de la representación nacional. La exposición de motivos del proyecto, señala que "*la Ley de Inteligencia que se propone y de la cual no hay antecedentes, sea elaborada con un amplio acuerdo político y técnico, en tanto definirá aspectos sensibles para la seguridad y defensa nacionales, así como para las garantías democráticas de los ciudadanos*".

### *Venezuela*

En Venezuela hubo un frustrado intento de sanción de la controvertida Ley de Inteligencia durante el año 2008, caricaturizada como *ley sapo*,<sup>122</sup> de muy bajos estándares en materia de garantías constitucionales y judiciales, lo que motivó su posterior derogación por el propio gobierno bolivariano del mandatario Hugo Chávez. Luego fue creado un nuevo organismo de inteligencia, el Servicio Bolivariano de Inteligencia (SEBIN),<sup>123</sup> que reemplaza a la policía política de la antigua Dirección de los Servicios de Inteligencia y Prevención (DISIP), mediante Decreto N° 7453 de junio del 2010. Dejamos constancia de las asombrosas similitudes, en estilo, fondo y forma, de la normatividad de inteligencia de la República Bolivariana de Venezuela, generada por el Presidente Hugo Chávez, con la del Perú de los años noventa con Alberto Fujimori en el poder y Vladimiro Montesinos como jefe real del SIN.<sup>124</sup>

### *Bolivia*

En este país ha sido preparado un ante-Proyecto de Ley, a inicios del año 2010 para la creación de una Dirección de Inteligencia del Estado Plurinacional (DIDEP), como nuevo e inédito organismo de inteligencia en el nivel político-estratégico para la toma de decisiones. Conforme a este ante-Proyecto se contempla el control interno a través de la Unidad de Auditoría Interna, la Fiscalización de las actividades de inteligencia corresponde a la Asamblea Legislativa Plurinacional a través de una Comisión Especial, y la fiscalización administrativa correspondería a la Contraloría General del Estado. Se garantiza la protección de los derechos fundamentales y garantías civiles y políticas; y no se podrá realizar tareas represivas sin autorización judicial. Actualmente, la

policía y las fuerzas armadas asumen los roles de inteligencia dentro de cada uno de sus sectores.

### Conclusiones

Referente a la pregunta inicial del presente trabajo, podemos concluir que la tendencia en materia de inteligencia latinoamericana se orienta hacia su empleo descentralizado a través de los mecanismos de controles externos (controles parlamentarios, judiciales y económico-financieros) bajo regímenes democráticos, conforme a las iniciativas parlamentarias (como en el caso de Perú elaborado aquí) que introdujo modificaciones legales que permitieron la dación de la vigente ley N° 28664. Sin embargo, en Colombia el caso del Inspector General de la Dirección Nacional de Inteligencia, genera una iniciativa para sustentar un control *interno* y autónomo a los servicios de inteligencia.

La evolución de los modelos de organismos de inteligencia centralizadores y los organismos descentralizadores (que incluyen la introducción de mecanismos de controles) ha sido el fruto de una evolución desde los tiempos en que se trasgredían los derechos de las personas, hasta hoy en día en que los citados mecanismos de controles externos permiten que las actividades de inteligencia sean más acordes con las tendencias democráticas; esta evolución se debió principalmente a los procesos reorganizativos que han sufrido cada uno de los organismos de inteligencia de la región.<sup>125</sup>

A raíz de la reorganización de los organismos de inteligencia, se consideró establecer Comisiones Reformadoras que busquen institucionalizar los cambios democráticos requeridos en dicha materia. El balance es positivo, ya que se puede apreciar en las legislaciones vigentes la introducción de controles democráticos (mecanismos de controles externos: parlamentarios, judiciales y económico-financieros)<sup>126</sup> que posibilitan el respeto a los derechos humanos, que requieren de autorizaciones judiciales para “operaciones especiales”, y cuyos organismos de inteligencia están sometidos a diversos mecanismos de controles. La constitución de estas Comisiones permite institucionalizar los procesos de reorganizaciones dentro de cada uno de los organismos de inteligencia a través de la discusión y el debate público que garantice el *control social*<sup>127</sup> a través de la población y de la opinión pública.

En suma, ante las amenazas y riesgos todavía existentes en el Perú creemos, que particularmente en la guerra contra el narcotráfico y los remanentes asociados

## Gestión de Inteligencia en las Américas

del terrorismo,<sup>128</sup> así como contra el crimen organizado, se aprecia la resolución de la tensión entre la descentralización de inteligencia a través de los citados mecanismos de controles externos y la aplicación de una autogestión eficaz del trabajo secreto preventivo.

### Adenda

Con posterioridad a la elaboración de este trabajo, el poder ejecutivo del Perú, bajo el amparo de Facultades Delegadas otorgadas por el Congreso de la República, mediante la Ley N° 29915 sobre *Reforma del Sistema de Seguridad y Defensa Nacional* del 12 de septiembre de 2012, promulgó durante el mes de diciembre de 2012, el Decreto Legislativo N° 1141 de *Fortalecimiento y Modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia - DINI*. Así, se produce una suerte de *ricorsi* de política legislativa en el Perú, al regularse nuevamente, tal como lo fue en los años 1984 y 1991, por intermedio de Decretos Legislativos al conjunto de toda la inteligencia nacional. Debe recordarse que las dos últimas leyes de inteligencia existentes en el Perú, la Ley Ordinaria Congresal N° 27479 del 2001 y la Ley Ordinaria Congresal N° 28664 del 2006, fueron diseñadas, elaboradas y aprobadas enteramente desde el Parlamento nacional, siguiendo todos los pasos que establece el procedimiento parlamentario común para la elaboración de dichas Leyes Ordinarias.

La idea de formular cambios a la normatividad de inteligencia se incubaría en la Comisión de Inteligencia del Congreso de la República,<sup>129</sup> al iniciarse el proceso congresal 2011-2016, y particularmente, en la Primera Legislatura, para el período 2011-2012, bajo la Presidencia de la Comisión de Inteligencia del Congresista José Urquiza Maggia (Partido Nacionalista/GANA PERU, de la bancada oficialista), quien presentó durante el mes de enero del 2012 un paquete de cinco (5) Proyectos de Ley<sup>130</sup> para modificar la Ley de Inteligencia N° 28664 por entonces vigente. Todos los planteamientos propuestos en los citados Proyectos de Ley fueron insertados en el flamante Decreto Legislativo N° 1141.

En líneas generales podemos señalar que, a nuestro entender, resulta conveniente que el nuevo Decreto Legislativo N° 1141 promulgado—el mismo que contiene 6 títulos y 43 artículos—<sup>131</sup> deje intactos y sin mayor variación los controles públicos o denominados "democráticos", particularmente el legislativo

y judicial, y los principios que regulan a la actividad de inteligencia, recogiendo en ese sentido la letra y espíritu de su antecesora, la Ley Ordinaria N° 28664 del 2006. El nuevo Decreto Legislativo N° 1141 también recoge la línea establecida en su antecesora (la Ley N° 28664) de mantener un *Glosario*, o conceptos de inteligencia, con la idea de mejorar la operatividad del Sistema de Inteligencia y establecer claramente las competencias, funciones y objetivos de cada uno de todos los entes que la conforman (artículo 2º, "Definiciones" del Decreto Legislativo N° 1141). Es lo que se valoró en su momento, producto de la experiencia incluida en el texto de la Ley argentina N° 25520 del 2001 y que las leyes peruanas de inteligencia históricamente no contenían.

Otro aspecto que merece destacarse en el nuevo Decreto es su Título V; *Medidas de protección del Personal de Inteligencia y de la Actividad de Contrainteligencia* (artículos 38, 39 40 y 41). Dicha propuesta también sería plasmada, con matices diferentes, y más bien ampliados, con posterioridad, en el Proyecto de Ley 724/2011-CR que propone establecer el *Garantizar la integridad física y seguridad del personal que participa en actividades de Inteligencia y contrainteligencia*, que fue presentado el 10 de enero del 2012 en el Congreso. Debe recordarse, que en el contexto peruano de amenazas latentes, reales y potenciales, referidas al narcotráfico, el terrorismo y el crimen organizado, resulta muy necesario que el personal de inteligencia pueda disponer de un amparo y respaldo, a través de mecanismos muy específicos de protección legal, para el desempeño de sus complicadas labores, especialmente en la tarea recolección de información efectuada por fuente humana (HUMINT): en Latinoamérica, y su derecho comparado generado sobre la materia, Panamá (Decreto Ley N° 9, que creó la Secretaría Nacional de Inteligencia y Seguridad) y Colombia (Ley N° 1288) avanzaron en respectivos sus textos legales, con redacciones bastante similares, en esa dirección, durante los años 2008 y 2009 respectivamente.

En suma reiteramos nuestro postulado en el sentido que proseguimos transitando dentro de un escenario y proceso histórico sumamente complejo, especialmente reciente, de la inteligencia peruana, caracterizado por luces y sombras, y que en la hora y tiempo presente dispone de una nueva ley de forma de decreto legislativo – producto de un proceso innovador.<sup>132</sup>

## Gestión de Inteligencia en las Américas

Tabla 2 Comparación de Legislación de Inteligencia Vigente y Derogada en Perú	
<b>Decreto Legislativo N° 1141</b> (vigente desde 11 diciembre 2012)	<b>Ley N° 28664</b> (derogada-vigente 20 enero 2006 hasta 11 diciembre 2012)
TÍTULO I DISPOSICIONES GENERALES  CAPÍTULO I OBJETO, DEFINICIONES Y PRINCIPIOS DE LA ACTIVIDAD DE INTELIGENCIA	TÍTULO I DISPOSICIONES GENERALES  CAPÍTULO I OBJETO, DEFINICIONES Y PRINCIPIOS DE LA ACTIVIDAD DE INTELIGENCIA
<p><b>Artículo 1.- Objeto</b>                      El presente Decreto Legislativo establece el marco jurídico que regula la finalidad, principios, organización, atribuciones, funciones, coordinación, control y fiscalización, que deben observar los componentes del SINA y los que señalen esta norma.</p>	<p><b>Artículo 1.- Objeto de la Ley</b>                      La presente Ley establece el marco jurídico que regula la finalidad, principios, organización, atribuciones, funciones, coordinación, control y fiscalización de las actividades de inteligencia que ejecutan los organismos del Sistema de Inteligencia Nacional - SINA.</p> <p><b>Artículo 2.- Alcances y Límites</b>                      La presente Ley desarrolla los alcances y establece los límites que deben observar los organismos del Sistema de Inteligencia Nacional - SINA y las que señale la presente Ley.</p> <p><b>Artículo 3.- Objetivo de la actividad de inteligencia</b>                      La actividad de inteligencia tiene por objetivo proporcionar oportunamente a través del Órgano Rector del Sistema de Inteligencia Nacional - SINA, al Presidente Constitucional de la República y al Consejo de Ministros, el conocimiento útil, obtenido mediante el procesamiento de las informaciones, sobre las amenazas y riesgos actuales y potenciales, que puedan</p>

Tabla 2 , (continua) Comparación de Legislación de Inteligencia Vigente y Derogada en Perú	
Decreto Legislativo N° 1141 (vigente desde 11 diciembre 2012)	Ley N° 28664 (derogada-vigente 20 enero 2006 hasta 11 diciembre 2012)
	afectar la seguridad nacional y el ordenamiento constitucional de la República.
<b>Artículo 2.- Definiciones</b> Para los fines del presente Decreto Legislativo y de las actividades reguladas por el mismo, se entenderá por:	<b>DISPOSICIONES                      COMPLEMENTARIAS                      PRIMERA: GLOSARIO</b>
1) <b>Inteligencia:</b> Actividad que comprende un proceso sistemático de búsqueda, evaluación y análisis de información, cuya finalidad es producir conocimiento útil para la toma de decisiones.	12) <b>Inteligencia:</b> Conjunto de actividades basadas en un ciclo de producción consistente en la obtención, recolección, búsqueda, acopio y procesamiento y difusión de informaciones destinadas a un usuario o consumidor final, para la toma de decisiones en materia de seguridad nacional, con objeto de prevenir sobre amenazas, riesgos y oportunidades.
2) <b>Contrainteligencia:</b> Parte de la actividad de inteligencia que protege las capacidades propias y evita acciones de inteligencia de actores que representen amenazas para la seguridad.	5) <b>Contrainteligencia:</b> Conjunto de actividades estratégicas, operativas y normativas destinadas a proteger las capacidades nacionales propias frente a acciones de inteligencia de enemigos y adversarios a la seguridad nacional.
3) <b>Inteligencia Nacional:</b> Conocimiento útil para la formulación y ejecución de la política general de gobierno, proporcionado al Presidente Constitucional de la República y al Consejo de Ministros, con el objeto de garantizar la vigencia de los derechos humanos, proteger a la población de las amenazas contra su seguridad, defender la soberanía nacional, y promover el bienestar general y el desarrollo integral de la Nación. Además, comprende a la Inteligencia Militar e Inteligencia Policial.	

## Gestión de Inteligencia en las Américas

Tabla 2, (continua) Comparación de Legislación de Inteligencia Vigente y Derogada en Perú	
Decreto Legislativo N° 1141 (vigente desde 11 diciembre 2012)	Ley N° 28664 (derogada-vigente 20 enero 2006 hasta 11 diciembre 2012)
4) <b>Inteligencia Militar:</b> Conocimiento útil sobre las capacidades y vulnerabilidades del poder y potencial militar de actores de interés, para garantizar la independencia, soberanía, integridad territorial y el orden constitucional de la República.	
5) <b>Inteligencia Policial:</b> Conocimiento útil sobre las capacidades y vulnerabilidades de actores de interés, nacionales y extranjeros, para garantizar, mantener y restablecer el orden interno, orden público y la seguridad ciudadana, con la finalidad de preservar la gobernabilidad y el Estado de Derecho.	
6) <b>Canal de Inteligencia:</b> Conducto especial, exclusivo y seguro, por el que los distintos componentes del SINA intercambien información e inteligencia necesarias para garantizar la seguridad nacional.	4) <b>Canal de Inteligencia:</b> Es el mecanismo que asegura que los órganos componentes del Sistema de Inteligencia Nacional - SINA intercambien información, inteligencia y contra-inteligencia necesarias para garantizar la seguridad nacional.
7) <b>Apreciación de Inteligencia:</b> Estudio metodológico e integral de uno o más actores para resolver un problema de inteligencia. Se materializa en un documento cuyas conclusiones sirven para el planeamiento de las actividades de inteligencia en todo nivel.	
	1) <b>Campo:</b> Dominio, factor o variable sectorial de la seguridad nacional que comprende cuatro elementos centrales: el político, el económico, el social y/o psicosocial y el militar.



<b>Tabla 2, (continua)</b> <b>Comparación de Legislación de Inteligencia Vigente y Derogada en Perú</b>	
<b>Decreto Legislativo N° 1141</b> (vigente desde 11 diciembre 2012)	<b>Ley N° 28664</b> (derogada-vigente 20 enero 2006 hasta 11 diciembre 2012)
	2) <b>Campo militar:</b> Dominio, factor o variable de la seguridad nacional en la que el componente castrense propiamente dicho y las fuerzas armadas se constituyen como los elementos centrales de la actividad.
	3) <b>Campo no militar:</b> Dominio, factor o variable de la seguridad nacional en la que los aspectos políticos, económicos y sociales se constituyen como los elementos centrales de la actividad.
	6) <b>Gastos reservados:</b> Son aquellos destinados a la adquisición, contratación y ejecución de bienes, servicios y obras de carácter secreto, que de hacerse en forma pública, pondría en riesgo la seguridad nacional, la integridad del personal de inteligencia o sus fuentes de información. Se clasifican en: <ul style="list-style-type: none"> <li>a) Los necesarios para adquirir el equipamiento imprescindible para la ejecución de las labores de inteligencia y contrainteligencia.</li> <li>b) Los necesarios para el desarrollo o adquisición de dispositivos inéditos para la ejecución de labores específicas de inteligencia o contrainteligencia.</li> <li>c) Los efectuados para el alistamiento y durante la obtención de información de fuente cerrada, y fuente abierta cuando lo amerite, en la ejecución de las labores de inteligencia y contrainteligencia.</li> </ul>

## Gestión de Inteligencia en las Américas

Tabla 2, (continua)	
Comparación de Legislación de Inteligencia Vigente y Derogada en Perú	
Decreto Legislativo N° 1141 (vigente desde 11 diciembre 2012)	Ley N° 28664 (derogada-vigente 20 enero 2006 hasta 11 diciembre 2012)
	<p>7) <b>Información:</b> Todo acto que revela dichos, situaciones y acciones sobre hechos que han acontecido, acontecen o acontecerán; para comunicar o adquirir conocimientos que permitan ampliar o precisar los que se poseen sobre una materia determinada.</p>
	<p>13) <b>Inteligencia Estratégica:</b> Fase y producto final del ciclo de inteligencia, cuyo objeto es constituirse en insumos en el proceso de toma de decisiones en el más alto nivel gubernamental, en función de prevenir y alertar sobre amenazas, riesgos y oportunidades para la seguridad nacional.</p>
	<p>14) <b>Operaciones especiales:</b> Acciones operativas de inteligencia y contrainteligencia, que suponen la transgresión de determinados derechos ciudadanos, en razón de amenazas a la seguridad nacional, requiriendo previa autorización judicial para su realización.</p>
	<p>15) <b>Recursos especiales:</b> Los recursos especiales son las asignaciones económicas que efectúa el Ministerio de Economía y Finanzas bajo el Régimen de Ejecución Especial para atender los gastos de naturaleza reservada.</p>
	<p>16) <b>Seguridad Nacional:</b> Condición de viabilidad, estabilidad, continuidad y bienestar del Estado y la Nación, a través de políticas públicas especializadas sectoriales de defensa y orden interno, inteligencia y en campos o dominios no militares;</p>

Tabla 2, (continua)	
Comparación de Legislación de Inteligencia Vigente y Derogada en Perú	
Decreto Legislativo N° 1141 (vigente desde 11 diciembre 2012)	Ley N° 28664 (derogada-vigente 20 enero 2006 hasta 11 diciembre 2012)
	para protegerlo y ponerlo fuera de peligro, ante situaciones de amenaza, daño potencial o riesgo.
<p><b>Artículo 3.- Principios de la actividad de inteligencia</b> Las actividades de inteligencia se sustentan en los siguientes principios:</p>	<p>TÍTULO I DISPOSICIONES GENERALES CAPÍTULO I OBJETO, ALCANCES Y LÍMITES DE LA LEY; OBJETIVO Y PRINCIPIOS DE LA ACTIVIDAD DE INTELIGENCIA</p> <p><b>Artículo 4.- Principios de la actividad de inteligencia</b> Las actividades de inteligencia se sustentan en los siguientes principios:</p>
1) <b>Legalidad:</b> Los componentes del SINA, en el cumplimiento de sus funciones respetan la Constitución Política del Perú y las Leyes.	1) <b>Legalidad:</b> Los componentes del Sistema de Inteligencia Nacional - SINA, en el cumplimiento de sus funciones respetan la Constitución y las Leyes. Las operaciones especiales sólo se efectúan con autorización de la autoridad competente prevista en la presente Ley.
2) <b>Legitimidad:</b> Las actividades de inteligencia se legitiman en razón de la seguridad nacional, respetando el equilibrio entre las necesidades del Estado y los derechos de las personas y el respeto a la ley.	2) <b>Legitimidad:</b> Las actividades de inteligencia se legitiman respetando el equilibrio entre las necesidades del Estado y los derechos de las personas; entre la eficiencia para la obtención de la información y el respeto a la Ley; entre el control y la discrecionalidad; y, entre la magnitud de la amenaza y/o el riesgo y la proporcionalidad de los medios empleados según el caso.

## Gestión de Inteligencia en las Américas

Tabla 2, (continua)	
Comparación de Legislación de Inteligencia Vigente y Derogada en Perú	
Decreto Legislativo N° 1141 (vigente desde 11 diciembre 2012)	Ley N° 28664 (derogada-vigente 20 enero 2006 hasta 11 diciembre 2012)
3) <b>Control democrático:</b> La naturaleza reservada de las actividades de inteligencia requiere el control especializado de otras instancias del Estado, señaladas en el presente Decreto Legislativo.	3) <b>Control democrático:</b> La naturaleza reservada de las actividades de inteligencia requiere el control especializado de otras instancias del Estado, señaladas en la presente Ley.
4) <b>Pertinencia:</b> La inteligencia que se proporciona debe ser útil para la adecuada toma de decisiones. Se entiende por útil cuando satisface oportunamente las necesidades de información.	4) <b>Pertinencia:</b> Para la toma de decisiones vinculadas al desarrollo de los intereses y objetivos nacionales; y las amenazas y riesgos actuales y potenciales que afecten la seguridad nacional, la inteligencia se brinda en forma preventiva y oportuna.
5) <b>Circulación restringida:</b> El conocimiento de las actividades de inteligencia es restringido. La divulgación de inteligencia está circunscrita a las entidades públicas autorizadas, en las condiciones previstas en el presente Decreto Legislativo.	5) <b>Circulación restringida:</b> El conocimiento de las actividades de inteligencia es restringido. La divulgación de inteligencia está circunscrita a las entidades públicas autorizadas, en las condiciones previstas en la presente Ley.
6) <b>Especialidad:</b> Cada componente del SINA produce inteligencia especializada en materia de su estricta competencia, evitando la duplicidad de funciones.	6) <b>Especialidad:</b> Cada componente del Sistema de Inteligencia Nacional - SINA produce información especializada en materia de su estricta competencia, evitando la duplicidad de funciones.
7) <b>Planificación:</b> Las acciones del SINA son planificadas y debidamente presupuestadas para cumplir los objetivos, estrategias y responsabilidades previstos en el Plan de Inteligencia Nacional - PIN y los Planes Institucionales de Inteligencia - PII.	7) <b>Planificación:</b> Las acciones del Sistema de Inteligencia Nacional - SINA son planificadas y corresponden a los lineamientos del Plan Anual de Inteligencia - PAI.
8) <b>Exclusividad:</b> La ejecución de las actividades de inteligencia a que se refiere este Decreto Legislativo, está reservada únicamente a los componentes del SINA.	

Tabla 2, (continua) Comparación de Legislación de Inteligencia Vigente y Derogada en Perú	
Decreto Legislativo N° 1141 (vigente desde 11 diciembre 2012)	Ley N° 28664 (derogada-vigente 20 enero 2006 hasta 11 diciembre 2012)
CAPÍTULO II INFORMACIÓN CLASIFICADA	TÍTULO II SISTEMA DE INTELIGENCIA NACIONAL - SINA
<p><b>Artículo 4.- Información clasificada de inteligencia: reserva y manejo</b></p> <p>4.1 Es información clasificada de inteligencia, con el nivel de Secreto, aquella que poseen y/o generan los componentes del SINA, y que por su naturaleza y contenido constituye una excepción al ejercicio del derecho de acceso a la información pública, en razón de la seguridad nacional, de conformidad con lo establecido en la Ley de Transparencia y Acceso a la Información Pública.</p> <p>4.2 Adicionalmente, es información clasificada de inteligencia:</p> <p>a) El detalle de los recursos especiales asignados a los componentes del SINA.</p> <p>b) Las resoluciones que autorizan viajes al exterior de personal del SINA.</p>	CAPÍTULO II INFORMACIÓN CLASIFICADA Y DELITO
	<p><b>Artículo 14.- De la información clasificada</b></p> <p>14.1 La categoría de clasificación de la información que producen los componentes del Sistema de Inteligencia Nacional - SINA se efectúa en estricta aplicación de la Ley de Transparencia y Acceso a la Información Pública y lo normado en la presente Ley.</p> <p>14.2 Cualquier otro tipo de clasificación, fuera de lo estrictamente normado, invalida la clasificación, constituyendo información pública.</p>
	DISPOSICIONES COMPLEMENTARIAS PRIMERA: GLOSARIO
	<p>8) <b>Información clasificada:</b> Es aquella contenida en cualquier medio, que por razones de seguridad nacional requiere de un tratamiento diferenciado de la información de carácter público; y cuyo conocimiento es restringido a los funcionarios o autoridades del Estado autorizados expresamente por ley. Las únicas categorías de clasificación son las previstas en la Ley</p>

## Gestión de Inteligencia en las Américas

Tabla 2, (continua) Comparación de Legislación de Inteligencia Vigente y Derogada en Perú	
Decreto Legislativo N° 1141 (vigente desde 11 diciembre 2012)	Ley N° 28664 (derogada-vigente 20 enero 2006 hasta 11 diciembre 2012)
	<p>de Transparencia y Acceso a la Información Pública, a saber: Secreta, Reservada y Confidencial.</p> <p>9) <b>Información confidencial:</b> Es aquella que contiene consejos, recomendaciones u opiniones, producidas como parte del proceso deliberativo y consultivo previo a la toma de una decisión de gobierno, que comprometa la seguridad nacional.</p> <p>10) <b>Información reservada:</b> Es aquella que estando en los ámbitos del orden interno, las relaciones exteriores y los procesos de negociaciones internacionales, su revelación originaría riesgos a la seguridad nacional.</p> <p>11) <b>Información secreta:</b> Es aquella que estando referida al ámbito militar, tanto en lo externo e interno de la defensa nacional; su revelación originaría riesgo a la seguridad nacional.</p>
4.3 Son responsables de la correcta clasificación de la información el titular del sector o pliego al que corresponda el componente del SINA o los funcionarios designados por éste.	<p><b>Artículo 14.- De la información clasificada</b></p> <p>14.3 Son responsables de la correcta clasificación de la información el titular del sector o pliego respectivo o los funcionarios designados por éste.</p>
4.4 Los funcionarios y demás personal de los componentes del SINA y de las instituciones que por razones de función tomen conocimiento de información clasificada de inteligencia, están obligados a guardar reserva y mantener su	<p><b>Artículo 16.- Obligación de guardar secreto</b></p> <p>Los funcionarios y demás personal de los componentes del Sistema de Inteligencia Nacional - SINA y de las instituciones que por razones funcionales tomen conocimiento de algún expediente</p>

Tabla 2, (continua) Comparación de Legislación de Inteligencia Vigente y Derogada en Perú	
<b>Decreto Legislativo N° 1141</b> (vigente desde 11 diciembre 2012)	<b>Ley N° 28664</b> (derogada-vigente 20 enero 2006 hasta 11 diciembre 2012)
carácter de secreto aún después del término de sus funciones, hasta su desclasificación, bajo responsabilidad.	o contenido de los archivos del Sistema de Inteligencia Nacional - SINA, están obligados a guardar reserva y mantener el carácter clasificado de su existencia y contenido aun después del término de sus funciones.
<b>Artículo 5.- Acceso de la información</b> En uso de sus funciones de control y fiscalización, las autoridades, funcionarios o instituciones autorizados por ley, pueden solicitar el acceso a información clasificada de inteligencia a los componentes del SINA; la que será proporcionada con obligatorio conocimiento de la Dirección Nacional de Inteligencia.	<b>Artículo 15.- Acceso a la información, manejo y delito</b> 15.1 En uso de sus funciones de control y fiscalización, las autoridades, funcionarios o instituciones autorizados por Ley, solicitan información clasificada; la que se proporciona por los componentes del Sistema de Inteligencia Nacional - SINA, bajo responsabilidad.  15.2 La información clasificada, proporcionada a las autoridades, funcionarios o instituciones autorizadas por Ley, no puede ser divulgada, revelada, ni reproducida bajo ningún medio.  15.3 Las autoridades, funcionarios o instituciones autorizados por Ley a conocer información clasificada, que divulguen, revelen y/o hagan accesible su contenido, cometen delito.
<b>Artículo 6.- Desclasificación de la información</b> 6.1 La desclasificación de información clasificada, producida por el SINA, relativa a la seguridad nacional, procede a los veinte (20) años.	<b>Artículo 17.- Desclasificación de información clasificada</b> 17.1 La desclasificación de información clasificada, producida por el Sistema de Inteligencia Nacional - SINA, relativa a la seguridad nacional, procede conforme a los siguientes plazos: a) La información confidencial a los diez (10) años de clasificada.

## Gestión de Inteligencia en las Américas

Tabla 2, (continua) Comparación de Legislación de Inteligencia Vigente y Derogada en Perú	
Decreto Legislativo N° 1141 (vigente desde 11 diciembre 2012)	Ley N° 28664 (derogada-vigente 20 enero 2006 hasta 11 diciembre 2012)
	b) La Información reservada a los quince (15) años de clasificada.  c) La información secreta a los veinte (20) años de clasificada.  <b>Artículo 18.- Sanciones</b> La inobservancia de lo normado en el Capítulo II del Título II de la presente Ley, por las personas señaladas en los respectivos artículos, se sanciona conforme a las leyes y reglamentos aplicables.  <b>Artículo 19.- Destrucción de información innecesaria</b> Toda información obtenida para la producción de inteligencia por el Sistema de Inteligencia Nacional -SINA, que sea innecesaria para el objetivo del sistema por corresponder a los derechos fundamentales de la persona humana y a la esfera de su vida privada, debe ser destruida por los funcionarios responsables de los componentes del sistema que la detenten, bajo responsabilidad de inhabilitación y sin perjuicio de las sanciones civiles y/o penales que correspondan.
6.2 Transcurrido el plazo señalado en el numeral anterior, cualquier ciudadano peruano puede solicitar la información clasificada de inteligencia, la cual podrá ser entregada si el titular del sector o pliego al que corresponde el componente del Sistema de Inteligencia Nacional -SINA, con opinión favorable del Director de Inteligencia Nacional, considera que su divulgación no constituye	



Tabla 2, (continua) Comparación de Legislación de Inteligencia Vigente y Derogada en Perú	
Decreto Legislativo N° 1141 (vigente desde 11 diciembre 2012)	Ley N° 28664 (derogada-vigente 20 enero 2006 hasta 11 diciembre 2012)
<p>riesgo para la seguridad de las personas, integridad territorial y/o subsistencia del sistema democrático. En caso contrario, deberá fundamentar expresamente y por escrito las razones para que continúe la clasificación y el período que considera que debe continuar clasificado. El documento que fundamenta que la información continua clasificada, en el plazo de diez (10) días, se pone en conocimiento de la Comisión de Inteligencia del Congreso de la República y del Consejo de Ministros, la que puede ordenar su desclasificación.</p>	
<p>6.3 El titular del sector o pliego al que corresponde el componente del SINA puede renovar la clasificación por un nuevo período, informando al Director de Inteligencia Nacional y al Consejo de Ministros, el cual puede ordenar su desclasificación.</p>	
<p>6.4 Sólo invocando y fundamentando interés nacional y/o público, cualquier ciudadano peruano puede solicitar la desclasificación de información de inteligencia antes del vencimiento del plazo. El Presidente del Consejo de Ministros y el Ministro del sector al que pertenece el componente del Sistema de Inteligencia Nacional -SINA, de estimarlo pertinente y con opinión del Director de Inteligencia Nacional, proceden mediante decreto supremo a la desclasificación de la información.</p>	<p>17.2 Sólo invocando y fundamentando interés nacional y/o público, se puede solicitar la desclasificación de información clasificada antes de vencer el plazo respectivo. El sector correspondiente se pronuncia a más tardar dentro de los treinta (30) días de presentada la solicitud.</p> <p>17.3 El Presidente del Consejo de Ministros y el Ministro del sector al que pertenece el componente del Sistema de Inteligencia Nacional - SINA, mediante decreto supremo, proceden a la desclasificación de la información.</p>

## Gestión de Inteligencia en las Américas

Tabla 2 LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: SISTEMA DE INTELIGENCIA NACIONAL - SINA	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
TÍTULO II SISTEMA DE INTELIGENCIA NACIONAL - SINA  CAPÍTULO I DEFINICIÓN, OBJETIVOS Y ESTRUCTURA DEL SINA Y PLAN DE INTELIGENCIA NACIONAL - PIN	TÍTULO II SISTEMA DE INTELIGENCIA NACIONAL - SINA  CAPÍTULO I DEFINICIÓN Y ORGANIZACIÓN DEL SISTEMA DE INTELIGENCIA NACIONAL - SINA
<p><b>Artículo 7.- Definición del SINA</b></p> <p>7.1 El SINA es el conjunto de principios, normas, procedimientos, técnicas, instrumentos, organismos y órganos del Estado funcionalmente vinculados, que bajo la dirección y coordinación de la Dirección Nacional de Inteligencia - DINI como ente rector, producen Inteligencia Nacional, Inteligencia Militar e Inteligencia Policial, y ejecutan medidas de contrainteligencia en las áreas de su responsabilidad.</p>	<p><b>Artículo 5.- Definición</b></p> <p>5.1 El SINA es el conjunto de instituciones del Estado funcionalmente vinculados, que actúan coordinadamente en la producción de inteligencia y ejecución de medidas de contrainteligencia, para la toma de decisiones, frente a las amenazas y/o riesgos actuales y potenciales contra la seguridad nacional.</p>
<p>7.2 Los componentes del SINA intercambian información vía el canal de inteligencia.</p>	<p>5.3 Los componentes que conforman el SINA, sin perjuicio de sus dependencias y deberes respecto de los superiores jerárquicos de las instituciones a las que pertenecen, se relacionan entre sí bajo la dirección del Órgano Rector, a través del intercambio de información, vía el canal de inteligencia y la cooperación mutua.</p>

<b>Tabla 2, (continua)</b> <b>LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección:</b> <b>SISTEMA DE INTELIGENCIA NACIONAL - SINA</b>	
<b>Decreto Legislativo N° 1141 (vigente)</b>	<b>Ley N° 28664 (derogada)</b>
7.3 El SINA forma parte del Sistema de Defensa Nacional y mantiene relaciones técnicas de coordinación con la Secretaría de Seguridad y Defensa Nacional - SEDENA.	5.2 El SINA forma parte del Sistema de Seguridad Nacional.
<b>Artículo 8.- Objetivos</b> El SINA tiene los siguientes objetivos:  8.1 Producir el conocimiento útil para el proceso de toma de decisiones en materia de seguridad nacional.  8.2 Proteger las capacidades nacionales y evitar acciones de inteligencia de actores que representen amenazas a la seguridad nacional.	
<b>Artículo 9.- Estructura del SINA</b> El SINA está conformado por los siguientes componentes:  9.1 Consejo de Inteligencia Nacional - COIN	<b>Artículo 6.- Estructura del Sistema de Inteligencia Nacional - SINA</b> 6.1 La estructura del SINA está compuesta por:  a) Consejo de Inteligencia Nacional - COIN
9.2 Dirección Nacional de Inteligencia - DINI	b) Dirección Nacional de Inteligencia - DINI
9.3 Órgano de Inteligencia del Sector Relaciones Exteriores: -Dirección General de Asuntos Multilaterales y Globales del Ministerio de Relaciones Exteriores	e) La Dirección General de Asuntos de Seguridad y Defensa del Ministerio de Relaciones Exteriores

## Gestión de Inteligencia en las Américas

Tabla 2, (continua) LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: SISTEMA DE INTELIGENCIA NACIONAL - SINA	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
9.4 Órganos de Inteligencia del Sector Defensa:  - Segunda División del Estado Mayor Conjunto de las Fuerzas Armadas  - Dirección de Inteligencia del Ejército del Perú  - Dirección de Inteligencia de la Marina de Guerra del Perú  - Dirección de Inteligencia de la Fuerza Aérea del Perú	c) Los organismos de Inteligencia del sector Defensa
9.5 Órganos de Inteligencia del Sector Interior:  - Dirección General de Inteligencia del Ministerio del Interior  - Dirección de Inteligencia de la Policía Nacional del Perú	d) Los organismos de Inteligencia del sector Interior

Tabla 2, (continua) LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: SISTEMA DE INTELIGENCIA NACIONAL - SINA	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p><b>Artículo 10.- Plan de Inteligencia Nacional - PIN</b></p> <p>10.1 Para efectos del desarrollo de actividades de inteligencia y contrainteligencia, el SINA cuenta con el PIN, que contiene los objetivos, políticas, estrategias y responsabilidades de sus componentes, relacionados con las amenazas a la seguridad nacional y la identificación de oportunidades favorables a ella, siendo su cumplimiento de carácter obligatorio. Es aprobado por el Consejo de Seguridad y Defensa Nacional en abril del año anterior a su ejecución, a propuesta del ente rector del SINA.</p> <p>10.2 El presupuesto de los componentes del SINA comprende los fondos necesarios para cumplir y ejecutar los objetivos, políticas, estrategias y responsabilidades establecidos en el PIN.</p> <p>10.3 Cada componente del SINA elabora su Plan Institucional de Inteligencia - PII, en función de los objetivos, políticas, estrategias y responsabilidades establecidos en el PIN.</p>	

## Gestión de Inteligencia en las Américas

Tabla 2, (continua) LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: SISTEMA DE INTELIGENCIA NACIONAL - SINA	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p style="text-align: center;">CAPÍTULO II COMPONENTES DEL SINA</p> <p><b>Artículo 11.- Consejo de Inteligencia Nacional - COIN</b></p> <p>11.1 La reunión de los jefes de los componentes del SINA constituye la instancia consultiva y de coordinación técnica denominada Consejo de Inteligencia Nacional - COIN.</p>	<p>6.2 La reunión de los componentes del Sistema de Inteligencia Nacional constituye el Consejo de Inteligencia Nacional - COIN.</p> <p><b>Artículo 7.- Consejo de Inteligencia Nacional - COIN, composición y funciones</b></p> <p>7.1 El COIN es la máxima instancia colegiada del SINA, encargado de orientar las actividades de inteligencia y contrainteligencia. Tiene carácter deliberativo y resolutivo.</p> <p>7.2 El COIN es presidido por el Director Ejecutivo de la DINI, y lo integran:</p> <ul style="list-style-type: none"> <li>a) El Jefe de la Segunda División de Estado Mayor del Comando Conjunto de las Fuerzas Armadas - 2da. DIEMCFA.</li> <li>b) El Director General de Inteligencia del Ministerio del Interior - DIGIMIN.</li> <li>c) El Director de Inteligencia de la Policía Nacional del Perú - DIRIN.</li> <li>d) El Director General de Asuntos de Seguridad y Defensa del Ministerio de Relaciones Exteriores.</li> </ul>

<b>Tabla 2, (continua)</b> <b>LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección:</b> <b>SISTEMA DE INTELIGENCIA NACIONAL - SINA</b>	
<b>Decreto Legislativo N° 1141 (vigente)</b>	<b>Ley N° 28664 (derogada)</b>
<p>11.2 El Director de Inteligencia Nacional [de la DINI] es el presidente del COIN, que se reúne obligatoriamente una vez al mes y cada vez que su presidente lo requiera.</p>	<p>7.2 El COIN es presidido por el Director Ejecutivo de la DINI, y lo integran: (...)</p> <p><b>Artículo 27.- Jerarquía del Director Ejecutivo de la DINI</b>                      El Director Ejecutivo es el funcionario público de mayor jerarquía del SINA y preside el COIN.</p>
<p>11.3 Son funciones del COIN:</p> <p>11.3.1 Revisar el PIN propuesto por el ente rector.</p>	<p><b>Artículo 7.-</b>                      7.4 Son funciones del Consejo de Inteligencia Nacional - COIN:</p> <p>b) Revisar y dar su conformidad al Plan Anual de Inteligencia - PAI; luego de lo cual, lo remite para su aprobación por el Consejo de Seguridad Nacional el mismo que supervisa y evalúa su cumplimiento.</p>
<p>11.3.2 Revisar y opinar sobre los documentos de doctrina.</p> <p>11.3.3 Recomendar criterios y procedimientos técnicos comunes para los componentes del SINA.</p>	<p>c) Aprobar la doctrina, criterios y procedimientos necesarios para la operatividad común de los componentes del Sistema de Inteligencia Nacional - SINA.</p>
<p>11.3.4 Emitir opinión sobre las actividades de inteligencia consideradas en el PIN.</p>	<p>a) Deliberar y resolver la orientación de las actividades de inteligencia y contrainteligencia en función de las amenazas y/o riesgos contra la seguridad nacional y el Estado democrático de derecho.</p>
<p>11.3.5 Otras que le asigne el Director de Inteligencia Nacional.</p>	

## Gestión de Inteligencia en las Américas

Tabla 2, , (continua) LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: SISTEMA DE INTELIGENCIA NACIONAL - SINA	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
11.4 Participan en el COIN, a invitación del Director de Inteligencia Nacional, los funcionarios y las personas que se estimen pertinentes para el cumplimiento de los objetivos del SINA.	7.3 Participan en el Consejo de Inteligencia Nacional - COIN, a invitación, los Directores de Inteligencia de las fuerzas armadas; así como las personas y funcionarios que estimen pertinente para el objetivo del Sistema de Inteligencia Nacional - SINA.
<b>Artículo 12.- Ente rector</b> La Dirección Nacional de Inteligencia - DINI es el ente rector del SINA.	<b>Artículo 8.- Dirección Nacional de Inteligencia - DINI</b> 8.1 La Dirección Nacional de Inteligencia - DINI es el órgano rector especializado del SINA (...)
<b>Artículo 13.- Órgano de Inteligencia del Sector Relaciones Exteriores</b> 13.1 La Dirección General de Asuntos Multilaterales y Globales del Ministerio de Relaciones Exteriores:  13.1.1 Produce, coordina, centraliza, recolecta y canaliza la información relevante vinculada con los intereses y objetivos permanentes del Estado en el ámbito exterior, de conformidad con los lineamientos establecidos en el PIN.  13.1.2 Remite periódicamente la información requerida por el ente rector del SINA.  13.2 El Director General de Asuntos Multilaterales y Globales del Ministerio de Relaciones Exteriores debe acreditar calificación y experiencia en inteligencia.	<b>Artículo 11.- Dirección General de Asuntos de Seguridad y Defensa del Ministerio de Relaciones Exteriores</b> La Dirección General de Asuntos de Seguridad y Defensa del Ministerio de Relaciones Exteriores coordina, centraliza, recolecta, analiza y canaliza la información vinculada con los intereses y objetivos permanentes del Estado en el ámbito exterior.



Tabla 2, (continua) LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: SISTEMA DE INTELIGENCIA NACIONAL - SINA	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p><b>Artículo 14.- Órganos de Inteligencia del Sector Defensa</b></p> <p>14.1 Los órganos de inteligencia del Sector Defensa:</p> <p style="padding-left: 20px;">14.1.1 Producen inteligencia militar y realizan actividades de contrainteligencia en el campo de su especialidad, de conformidad con los lineamientos establecidos en el PIN.</p> <p style="padding-left: 20px;">14.1.2 Remiten periódicamente la información e inteligencia requerida por el ente rector del SINA.</p> <p>14.2 La Segunda División del Estado Mayor Conjunto de las Fuerzas Armadas dirige, orienta y coordina la producción de inteligencia para las operaciones militares, de conformidad con los lineamientos establecidos en el PIN.</p> <p>14.3 Los jefes de los Órganos de Inteligencia del Sector Defensa deben acreditar calificación y experiencia en inteligencia.</p>	<p><b>Artículo 9.- Organismos de Inteligencia del sector Defensa</b></p> <p>La Segunda División de Estado Mayor del Comando Conjunto de las Fuerzas Armadas dirige, coordina y centraliza los órganos de ejecución en la producción de inteligencia especializada para la defensa nacional en el campo o dominio militar.</p>
<p><b>Artículo 15.- Órganos de Inteligencia del Sector Interior</b></p> <p>15.1 Los Órganos de Inteligencia del Sector Interior:</p> <p style="padding-left: 20px;">15.1.1 Producen la inteligencia policily realizan actividades de contrainteligencia en el campo de su especialidad, de conformidad con los lineamientos establecidos en el PIN.</p>	<p><b>Artículo 10.- Organismos de Inteligencia del sector Interior</b></p> <p>10.1 La Dirección General de Inteligencia del Ministerio del Interior - DIGIMIN coordina y centraliza la inteligencia relacionada al orden interno, seguridad pública, seguridad ciudadana, crimen organizado y nuevas amenazas transnacionales, que produce la Dirección</p>

## Gestión de Inteligencia en las Américas

Tabla 2, (continua) LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: DIRECCIÓN NACIONAL DE INTELIGENCIA - DINI	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p>15.1.2 Remiten periódicamente la información e inteligencia requerida por el ente rector del SINA.</p> <p>15.2 La Dirección General de Inteligencia del Ministerio del Interior produce inteligencia para el SINA y las decisiones de la Alta Dirección del Ministerio del Interior, en el ámbito de su competencia.</p> <p>15.3 La Dirección de Inteligencia de la Policía Nacional del Perú produce inteligencia para el SINA y la Policía Nacional del Perú - PNP, en el marco del cumplimiento de su misión y funciones.</p> <p>15.4 El Director General de Inteligencia del Ministerio del Interior y el Director de Inteligencia de la Policía Nacional del Perú, deben acreditar calificación y experiencia en inteligencia.</p>	<p>de Inteligencia de la Policía Nacional y las informaciones que brindan las autoridades políticas.</p> <p>10.2 La Dirección de Inteligencia- DIRIN de la Policía Nacional tiene a su cargo la dirección y producción de inteligencia especializada dispuesta por su sector.</p>

Tabla 2 LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: DIRECCIÓN NACIONAL DE INTELIGENCIA - DINI	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p style="text-align: center;">TÍTULO III DIRECCIÓN NACIONAL DE INTELIGENCIA - DINI</p> <p style="text-align: center;">CAPÍTULO I ESTRUCTURA ORGÁNICA</p> <p><b>Artículo 16.- DINI</b> 16.1 La DINI es un organismo público ejecutor, con personería jurídica de derecho público, autonomía administrativa, funcional y económica; constituye pliego presupuestal propio. Su titular es el Director de Inteligencia Nacional.</p> <p>16.2 La DINI depende funcionalmente del Presidente de la República y se encuentra adscrita a la Presidencia del Consejo de Ministros.</p>	<p style="text-align: center;">TÍTULO III DIRECCIÓN NACIONAL DE INTELIGENCIA - DINI</p> <p style="text-align: center;">CAPÍTULO I FUNCIONES</p> <p><b>Artículo 23.- Órgano Rector del SINA</b> 23.1 La DINI es el Órgano Rector especializado del SINA; con personería jurídica de derecho público, autonomía administrativa, funcional y económica; constituye pliego presupuestal propio.</p> <p>23.2 La DINI depende funcionalmente del Presidente de la República y se encuentra adscrita a la Presidencia del Consejo de Ministros.</p> <p>23.3 Las auditorías y procedimientos de rendición de cuentas de los recursos asignados, incluyendo los recursos especiales, se rigen por lo dispuesto en la presente Ley.</p> <p><b>Artículo 8.- Dirección Nacional de Inteligencia - DINI</b> 8.1 La Dirección Nacional de Inteligencia - DINI es el órgano rector especializado del SINA (...)</p>
<p><b>Artículo 17- Funciones</b> <b>Son funciones de la DINI:</b></p> <p>17.1 Ejercer la rectoría del SINA.</p>	

## Gestión de Inteligencia en las Américas

Tabla 2, (continua) LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: DIRECCIÓN NACIONAL DE INTELIGENCIA - DINI	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
17.2 Producir Inteligencia Nacional para el Presidente de la República y el Consejo de Ministros para la formulación y ejecución de las acciones y políticas, con el objeto de garantizar la vigencia de los derechos humanos, defender la soberanía nacional, promover el bienestar general y el desarrollo integral de la Nación, y proteger a la población de las amenazas internas y externas contra su seguridad, en especial del accionar de organizaciones terroristas, del narcotráfico, del crimen organizado y otras, nacionales o extranjeras, que atenten o amenacen la plena vigencia del Estado democrático.	<b>Artículo 24.- Funciones de la DINI</b> Son funciones de la DINI: a) Proveer al Presidente Constitucional de la República y al Consejo de Ministros, la inteligencia y contrainteligencia necesaria, oportuna y predictiva para el proceso de toma de decisiones en materia de seguridad nacional.
17.3 Ejecutar actividades de contra-inteligencia en el ámbito de su competencia, en concordancia con los principios y objetivos de la actividad de inteligencia establecidos en el presente Decreto Legislativo.	<b>Artículo 8.-</b> 8.1 La DINI (...) tiene a su cargo la producción de inteligencia y ejecución de medidas de contrainteligencia, en los campos o dominios no militares de la seguridad nacional, en concordancia con los principios de la actividad de inteligencia establecidos en la presente Ley.
17.4 Consolidar las apreciaciones de inteligencia que remiten los componentes del SINA, para la elaboración del PIN.	<b>Artículo 24.-</b> b) Dirigir, coordinar, centralizar, integrar, procesar y difundir la inteligencia producida por los componentes del SINA, en concordancia con el Plan Anual de Inteligencia - PAI.
17.5 Formular el PIN y remitirlo al Consejo de Seguridad y Defensa Nacional para su aprobación.	c) Elaborar la propuesta de Plan Anual de Inteligencia - PAI, la misma que remite al COIN para su revisión y conformidad.

<b>Tabla 2, (continua)</b> <b>LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección:</b> <b>DIRECCIÓN NACIONAL DE INTELIGENCIA - DINI</b>	
<b>Decreto Legislativo N° 1141 (vigente)</b>	<b>Ley N° 28664 (derogada)</b>
	d) Articular los componentes del SINA en el COIN, empleando el canal de inteligencia, en estricta concordancia a la ejecución del Plan Anual de Inteligencia - PAI.
17.6 Dirigir, supervisar y controlar a los componentes del SINA, respecto al cumplimiento de lo establecido en el PIN.	<b>Artículo 8.-</b> 8.2 Es función de la DINI, dirigir, coordinar, centralizar, integrar, procesar y difundir la inteligencia que, con carácter obligatorio, le proveen todos los componentes del Sistema de Inteligencia Nacional SINA.
17.7 Asegurar el funcionamiento del canal de inteligencia en el SINA, en concordancia con los principios establecidos en el presente Decreto Legislativo.	8.3 Es responsabilidad del Órgano Rector asegurar el canal de inteligencia entre los componentes del Sistema de Inteligencia Nacional - SINA.
17.8 Constituir la autoridad técnica normativa a nivel nacional en materia de inteligencia y contrainteligencia.	
17.9 Supervisar y controlar el cumplimiento de sus normas técnicas.	<b>Artículo 24.-</b> g) Formular, ejecutar y evaluar el pliego presupuestal.
17.10 Establecer, por razones de seguridad nacional, oficinas de coordinación y designar funcionarios de enlace en los Ministerios y Organismos Públicos, cuyos titulares se sujetan a las normas técnicas establecidas para dicho fin.	
17.11 Informar a la Comisión de Inteligencia del Congreso de la República de acuerdo con lo establecido en el presente Decreto Legislativo.	<b>Artículo 24.-</b> e) Informar periódicamente a la Comisión de Inteligencia del Congreso de la República acerca de las actividades del SINA y cada vez que dicha Comisión lo requiera.

## Gestión de Inteligencia en las Américas

Tabla 2, (continua) LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: DIRECCIÓN NACIONAL DE INTELIGENCIA - DINI	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
17.12 Remitir periódicamente informes de gestión a la Presidencia del Consejo de Ministros sobre actividades de inteligencia y logro de metas.	a) Proveer al Presidente Constitucional de la República y al Consejo de Ministros, la inteligencia y contrainteligencia necesaria, oportuna y predictiva para el proceso de toma de decisiones en materia de seguridad nacional.
17.13 Establecer y fortalecer las relaciones de cooperación con organismos de inteligencia de otros países.	f) Establecer y fortalecer las relaciones de cooperación con organismos similares de otros países.
17.14 Formular su Plan Institucional de Inteligencia - PII.	
17.15 Aprobar y difundir los documentos de doctrina de inteligencia, cuyo contenido es de aplicación general por el SINA.  17.16 Capacitar y perfeccionar académicamente al personal del SINA.	<p><b>Artículo 13.- Estandarización de los componentes que conforman el SINA</b></p> <p>13.1 Los componentes del Sistema de Inteligencia Nacional - SINA estandarizarán los requisitos básicos y mínimos en sus procesos de selección y evaluación de sus recursos humanos; incidiendo en aspectos como experiencia en la materia, formación profesional, capacitación permanente, experiencia docente, evaluación psicológica y rendimiento profesional. La estandarización se aplica también en el campo de la doctrina y los procedimientos de trabajo.</p> <p>13.2 La evaluación del personal, doctrina y procedimientos de los componentes del SINA es periódica y permanente.</p>
17.17 Las demás establecidas por ley.	

<b>Tabla 2, (continua)</b> <b>LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección:</b> <b>DIRECCIÓN NACIONAL DE INTELIGENCIA - DINI</b>	
<b>Decreto Legislativo N° 1141 (vigente)</b>	<b>Ley N° 28664 (derogada)</b>
<b>Artículo 18.- Estructura orgánica</b> 18.1 El presente Decreto Legislativo establece la estructura básica de la DINI, cuyas funciones y atribuciones específicas se establecen en su Reglamento de Organización y Funciones.	CAPÍTULO II ORGANIZACIÓN  <b>Artículo 25.- Organización básica</b> 25.2 Las funciones de los órganos descritos precedentemente se detallan en el Reglamento de Organización y Funciones de la DINI.
18.2 La estructura orgánica básica de la DINI está compuesta por:  18.2.1 Alta Dirección: a. Dirección de Inteligencia Nacional b. Dirección Ejecutiva	25.1 La DINI tiene la siguiente organización:  a) Alta Dirección: a.1 Dirección Ejecutiva a.2 Subdirección
	b) Órganos de Asesoramiento: b.1 Oficina de Asesoría Jurídica b.2 Oficina de Planificación y Presupuesto
18.2.2 Órgano de Control Institucional	c) Órgano de Control: c.1 Oficina de Control Institucional
18.2.3 Órganos de Administración Interna	d) Órganos de Apoyo: d.1 Oficina de Administración d.2 Oficina de Soporte Técnico
18.2.4 Órganos de Línea	e) Órganos de Línea: e.1 Dirección de Inteligencia Estratégica e.2 Dirección de Contrainteligencia e.3 Dirección de Informaciones f) Órgano de Formación, Perfeccionamiento y Doctrina f.1 Escuela Nacional de Inteligencia (ENI)

## Gestión de Inteligencia en las Américas

Tabla 2, (continua) LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: DIRECCIÓN NACIONAL DE INTELIGENCIA - DINI	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p><b>Artículo 19.- Director de Inteligencia Nacional</b>                      El Director de Inteligencia Nacional es el funcionario público de mayor jerarquía de la DINI y del SINA. Es el titular de la DINI y su representante legal. Preside el Consejo de Inteligencia Nacional y asesora al Presidente de la República en asuntos de inteligencia.</p>	
<p><b>Artículo 20.- Requisitos para ser Director de Inteligencia Nacional</b>                      Para ser designado Director de Inteligencia Nacional se requiere:</p> <p>20.1 Ser peruano de nacimiento y no contar ni haber contado con otra nacionalidad.</p> <p>20.2 Tener expedito el ejercicio de la totalidad de sus derechos ciudadanos.</p> <p>20.3 Acreditar título profesional o grado académico de nivel universitario.</p> <p>20.4 Tener no menos de 35 años.</p> <p>20.5 No tener cargo político partidario alguno.</p> <p>20.6 Poseer conocimientos y experiencia en asuntos relacionados a seguridad, defensa y desarrollo nacional.</p> <p>20.7 No poseer antecedentes penales, judiciales ni policiales.</p>	<p><b>Artículo 28.- Requisitos para ser Director Ejecutivo</b>                      28.1 Para ser designado Director Ejecutivo se requiere:</p> <p>a) Ser peruano de nacimiento y no tener otra nacionalidad.</p> <p>b) Tener expedito el ejercicio de la totalidad de sus derechos ciudadanos.</p> <p>c) Acreditar título profesional o grado académico de nivel universitario.</p> <p>d) Tener no menos de 40 años.</p> <p>e) No tener cargo político partidario alguno.</p> <p>f) Poseer conocimientos y experiencia en asuntos relacionados a seguridad, defensa y desarrollo nacional.</p> <p>g) No poseer antecedentes penales, judiciales ni policiales vigentes.</p>



Tabla 2, (continua) LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: DIRECCIÓN NACIONAL DE INTELIGENCIA - DINI	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p><b>Artículo 21.- Designación y remoción del Director de Inteligencia Nacional</b>                      21.1 El Director de Inteligencia Nacional es designado y removido por el Presidente Constitucional de la República, mediante Resolución Suprema refrendada por el Presidente del Consejo de Ministros.</p>	<p><b>Artículo 26.- Designación y remoción del Director Ejecutivo y Subdirector de la DINI</b>                      26.1 El Director Ejecutivo (...) son designados y removidos por el Presidente Constitucional de la República, mediante Resolución Suprema refrendada por el Presidente del Consejo de Ministros.</p>
<p>21.2 Si el designado es miembro de las Fuerzas Armadas o de la Policía Nacional del Perú en situación de actividad, para ejercer el cargo debe previamente pasar a la situación de retiro.</p>	<p><b>Artículo 28.-</b>                      28.2 Si el designado por el Presidente Constitucional de la República es miembro de las Fuerzas Armadas o Policía Nacional en situación de actividad, para ejercer el cargo debe previamente solicitar su pase a la situación de retiro.</p>
<p>21.3 Si el designado es trabajador de la DINI, para ejercer el cargo debe previamente renunciar a la institución.</p>	
<p><b>Artículo 22.- Director Ejecutivo</b>                      22.1 El Director Ejecutivo es el segundo funcionario en jerarquía de la DINI. Es la máxima autoridad administrativa institucional. Ejerce sus funciones de conformidad con lo establecido en el Reglamento de Organización y Funciones de la DINI.                      22.2 Reemplaza al Director de Inteligencia Nacional en caso de ausencia o impedimento.</p>	

## Gestión de Inteligencia en las Américas

Tabla 2, (continua) LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: DIRECCIÓN NACIONAL DE INTELIGENCIA - DINI	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p><b>Artículo 23.- Requisitos para ser Director Ejecutivo</b>                      Para ser Director Ejecutivo de la DINI se deben reunir los mismos requisitos que para ocupar el cargo de Director de Inteligencia Nacional.</p>	<p><b>Artículo 29.- Requisitos para ser Subdirector de la DINI</b>                      29.1 Para ser designado Subdirector se requiere:</p> <ul style="list-style-type: none"> <li>a) Ser peruano de nacimiento y no tener otra nacionalidad.</li> <li>b) Tener expedito el ejercicio de la totalidad de sus derechos ciudadanos.</li> <li>c) Acreditar título profesional o grado académico de nivel universitario.</li> <li>d) Tener no menos de 40 años.</li> <li>e) No tener cargo político partidario alguno.</li> <li>f) Poseer conocimientos y experiencia en asuntos relacionados a seguridad, defensa y desarrollo nacional.</li> <li>g) No poseer antecedentes penales, judiciales ni policiales vigentes.</li> </ul> <p>29.2 Si el designado por el Presidente Constitucional de la República es miembro de las Fuerzas Armadas o Policía Nacional en situación de actividad, para ejercer el cargo debe previamente solicitar su pase a la situación de retiro.</p>
<p><b>Artículo 24.- Designación del Director Ejecutivo</b>                      El Director Ejecutivo es designado por el Presidente de la República mediante Resolución Suprema refrendada por el Presidente del Consejo de Ministros.</p>	<p><b>Artículo 26.- Designación y remoción del Director Ejecutivo y Subdirector de la DINI</b>                      26.1 El Director Ejecutivo y Subdirector de la DINI son designados y removidos por el Presidente Constitucional de la República, mediante Resolución Suprema refrendada por el Presidente del Consejo de Ministros.</p>

Tabla 2, (continua) LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: DIRECCIÓN NACIONAL DE INTELIGENCIA - DINI	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p><b>Artículo 25.- Sometimiento a investigaciones</b>                      El Director de Inteligencia Nacional y el Director Ejecutivo están sometidos en cuanto a su gestión a las investigaciones que puede iniciar el Poder Ejecutivo, el Poder Legislativo, el Poder Judicial, el Ministerio Público y la Contraloría General de la República.</p>	<p>26.2 En su calidad de funcionarios públicos, el Director Ejecutivo y el Subdirector están sometidos en cuanto a su gestión a las investigaciones que puede iniciar la propia administración pública, la Contraloría General de la República, el Ministerio Público, el Poder Judicial y el Poder Legislativo.</p>
<p>CAPÍTULO II PERSONAL DE INTELIGENCIA</p> <p><b>Artículo 26.- Personal de la DINI</b>                      26.1 El personal de la DINI se rige por el régimen de la actividad privada, conforme el Decreto Legislativo N° 728 y la normatividad que resulte aplicable.</p>	<p>CAPÍTULO III PERSONAL</p> <p><b>Artículo 33.- Personal de la DINI</b>                      El personal de la DINI se rige por el régimen de la actividad privada hasta la implementación de las normas que regulan la Carrera del Servidor Público y el Sistema de Remuneraciones del Empleo Público, conforme lo dispuesto en la Ley Marco del Empleo Público, Ley N° 28175.</p>
<p>26.2 Para pertenecer a la DINI se debe ser peruano por nacimiento y no contar ni haber contado con otra nacionalidad.</p>	
	<p>CAPÍTULO IV FORMACIÓN</p> <p><b>Artículo 34.- Escuela Nacional de Inteligencia - ENI</b>                      34.1 La ENI es el órgano académico encargado de la formación de personal de la DINI y de los analistas de inteligencia y personal de contrainteligencia del SINA.</p>

## Gestión de Inteligencia en las Américas

Tabla 2, (continua) LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: DIRECCIÓN NACIONAL DE INTELIGENCIA - DINI	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
	34.2 El Director de la ENI debe poseer como requisito mínimo el grado académico de Maestría y acreditar experiencia académica en el ámbito de inteligencia.
<p><b>Artículo 27.- Reserva de la información sobre el personal de la DINI</b>                      Las personas naturales o jurídicas que en razón de su función, deban acceder a la información contenida en los documentos de gestión y de personal de la Dirección Nacional de Inteligencia, deben guardar la reserva de su contenido, bajo responsabilidad.</p>	<p style="text-align: center;">TÍTULO II                      SISTEMA DE INTELIGENCIA NACIONAL - SINA</p> <p style="text-align: center;">CAPÍTULO I                      DEFINICIÓN Y ORGANIZACIÓN DEL SINA</p> <p><b>Artículo 12.- Obligación de informar (...)</b>                      12.5 La DINI, conjuntamente con la Unidad de Inteligencia Financiera del Perú - UIF, sus funcionarios y trabajadores, están sujetos al deber de reserva establecido por el artículo 12 de la Ley N° 27693 y sus modificatorias, así como a la obligación de guardar la reserva que dispone la presente Ley.</p>
<p style="text-align: center;">CAPÍTULO III                      RÉGIMEN ECONÓMICO Y FINANCIERO</p> <p><b>Artículo 28.- Régimen económico</b>                      28.1 El presupuesto de la DINI se financia con recursos que recibe del Tesoro Público y demás fuentes de financiamiento que se aprueben de acuerdo a la normatividad.                      28.2 También son recursos de la DINI:                      28.2.1 Los que reciba en donación o en virtud de convenios de cooperación</p>	<p style="text-align: center;">TÍTULO III                      DIRECCIÓN NACIONAL DE INTELIGENCIA - DINI</p> <p style="text-align: center;">CAPÍTULO V                      PRESUPUESTO, RÉGIMEN ECONÓMICO Y FINANCIERO</p> <p><b>Artículo 35.- Presupuesto</b>                      35.1 La Dirección Nacional de Inteligencia - DINI constituye pliego presupuestal propio.                      35.2 El Director Ejecutivo y el Subdirector son responsables por el uso</p>

Tabla 2, (continua) LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: DIRECCIÓN NACIONAL DE INTELIGENCIA - DINI	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p>técnica nacional y/o internacional de acuerdo con la normatividad vigente; y, 28.2.2 Otros que se establezcan por ley.</p>	<p>que se otorgue a los recursos asignados en el pliego presupuestal y los recursos especiales.</p> <p><b>Artículo 36.- Régimen económico</b>                      El presupuesto de la Dirección Nacional de Inteligencia - DINI se financia con recursos que recibe del Tesoro Público y demás fuentes de financiamiento incorporados por resolución del titular del pliego, los que reciba de donación o en virtud de convenios de cooperación técnica nacional e internacional; y otros que se establezcan por Ley.</p>
<p style="text-align: center;">CAPÍTULO V (debe decir "IV")                      CONTROL INSTITUCIONAL</p> <p><b>Artículo 29.- Control Institucional</b>                      29.1 El control de las actividades de gestión administrativa, económica y financiera de los recursos y bienes de los componentes del SINA son realizados por los Órganos de Control Institucional de las entidades correspondientes.                      29.2 El control sobre los recursos especiales por parte del Órgano de Control Institucional se efectúa, exclusivamente, verificando la legalidad en el fiel cumplimiento de las normas de la Directiva dispuesta en los artículos 29 y 30 del presente Decreto Legislativo.</p>	<p style="text-align: center;">CAPÍTULO II                      ORGANIZACIÓN</p> <p><b>Artículo 30.- Control Institucional</b>                      30.1 De acuerdo a lo dispuesto en la Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, el control de las actividades de gestión administrativa, económica y financiera de los recursos y bienes de los componentes del SINA son realizados en el caso de la DINI por la Oficina de Control Institucional; en el caso de los demás componentes del SINA por las Oficinas de Control Institucional de la instituciones a que corresponden.                      30.2 El control sobre los recursos especiales por parte de la Oficina de Control Institucional se efectúa, exclusivamente, verificando la legalidad en el fiel cumplimiento de las normas de la Directiva dispuesta en los artículos 31 y 32 de la presente Ley.</p>

## Gestión de Inteligencia en las Américas

Tabla 2, (continua) LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: DIRECCIÓN NACIONAL DE INTELIGENCIA - DINI	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p><b>Artículo 30.- Rendición de cuentas de recursos especiales</b></p> <p>30.1 Constituyen recursos especiales aquellos destinados a atender los gastos de naturaleza reservada de la actividad de inteligencia, que de hacerse en forma pública, pondrían en riesgo la seguridad nacional, la integridad del personal de inteligencia o sus fuentes de información. Los recursos especiales no pueden ser destinados para cubrir aumentos y/o pagos de haberes ordinarios y/o gastos de carácter personal, tanto del personal de la DINI como a cualquier personal de los componentes del SINA.</p> <p>30.2 El Director de Inteligencia Nacional establece bajo responsabilidad, mediante Directiva clasificada como secreta, el procedimiento para la autorización, ejecución, sustentación y control de la rendición de cuentas de los recursos especiales utilizados por el SINA; siendo sus disposiciones de obligatorio cumplimiento por todos los componentes del sistema.</p> <p>30.3 La Directiva debe contar con la previa opinión favorable de la Contraloría General de la República; requisito sin el que dicho documento no tiene efecto legal alguno.</p> <p>30.4 Es responsabilidad del Director de Inteligencia Nacional poner en conocimiento de los demás componentes del</p>	<p><b>Artículo 31.- Rendición de cuentas de recursos especiales</b></p> <p>31.1 El Director Ejecutivo de la DINI establece bajo responsabilidad, mediante Directiva clasificada como secreta, el procedimiento para la autorización, ejecución, sustentación y control de la rendición de cuentas de los recursos especiales utilizados por el SINA; siendo sus disposiciones de obligatorio cumplimiento por todos los componentes del sistema.</p> <p>31.2 La Directiva debe contar con la previa opinión favorable del Contralor General de la República; requisito sin el que dicho documento no tiene efecto legal alguno.</p> <p>31.3 El Contralor General de la República tiene un plazo improrrogable de treinta (30) días calendario, contados a partir de la recepción de la Directiva, para emitir pronunciamiento.</p> <p>Vencido el plazo sin pronunciamiento se entiende, por silencio administrativo positivo, que la Directiva cuenta con la opinión favorable correspondiente.</p> <p>31.4 Es responsabilidad del Director Ejecutivo poner en conocimiento de los demás componentes del SINA, la Directiva a que alude el presente artículo.</p> <p>31.5 Constituyen recursos especiales los que el Ministerio de Economía y Finanzas entrega para atender los gastos</p>

<b>Tabla 2, (continua)</b> <b>LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección:</b> <b>DIRECCIÓN NACIONAL DE INTELIGENCIA - DINI</b>	
<b>Decreto Legislativo N° 1141 (vigente)</b>	<b>Ley N° 28664 (derogada)</b>
<p>SINA, la Directiva a que alude el presente artículo.</p> <p>30.5 Los funcionarios y demás personal del Sistema Nacional de Control garantizan la debida reserva y el carácter de secreto de la información, de conformidad con lo establecido en el artículo 4° del presente Decreto Legislativo.</p> <p>30.6 La DINI deberá dar cuenta de uso de los gastos de naturaleza reservada de la actividad de inteligencia al Presidente del Consejo de Ministros por lo menos dos (2) veces al año.</p>	<p>reservados del proceso de inteligencia y la gestión de contrainteligencia.</p> <p>31.6 Los recursos especiales no pueden ser destinados para cubrir aumentos y/o pagos de haberes ordinarios tanto del personal de la DINI como a cualquier personal de los componentes del SINA.</p>
<p><b>Artículo 31.- Contrataciones que se efectúan con cargo a recursos especiales</b>                      Las contrataciones que se efectúen con cargo a los recursos especiales a que se refiere el artículo anterior, para actividades de inteligencia, que de hacerse en forma pública, pondrían en peligro la seguridad nacional, las fuentes de información o la integridad del personal de los componentes del SINA, tienen la clasificación de secreto y se rigen por la normativa de la materia.</p>	<p><b>Artículo 32.- Adquisiciones y Contrataciones</b>                      Las adquisiciones y contrataciones para actividades de inteligencia, que de hacerse en forma pública, pondrían en peligro la seguridad nacional, las fuentes de información o la integridad del personal de los componentes del SINA, tienen la clasificación de secreto y se rigen por la Directiva contemplada en el artículo precedente, no siéndole aplicable Ley especial alguna sobre la materia.</p>

## Gestión de Inteligencia en las Américas

TLEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: CONTROL DE LA ACTIVIDAD DE INTELIGENCIA	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p>TÍTULO IV CONTROL DE LA ACTIVIDAD DE INTELIGENCIA</p> <p>CAPÍTULO I CONTROL JUDICIAL</p>	<p>TÍTULO II SISTEMA DE INTELIGENCIA NACIONAL - SINA</p> <p>CAPÍTULO III CONTROL DE LA ACTIVIDAD DE INTELIGENCIA</p>
<p><b>Artículo 32.- Autorización judicial para procedimientos especiales de obtención de información</b> 32.1 Los procedimientos especiales de obtención de información son ejecutados exclusivamente por los componentes del SINA, se utilizan para acceder a información que resulta estrictamente indispensable para el cumplimiento de los objetivos de la actividad de inteligencia.</p>	<p>20.5 Las resoluciones del Vocal Superior Ad hoc autorizando operaciones especiales tienen carácter vinculante para todas las entidades públicas y privadas que deben coadyuvar a su realización, debiendo observar las disposiciones sobre información clasificada. El carácter vinculante de las resoluciones antes indicadas es excluyente respecto de la Unidad de Inteligencia Financiera del Perú-UIF-Perú, en tanto contravenga su autonomía funcional, técnica y administrativa.</p> <p>20.6 La solicitud motivada del Director Ejecutivo de la Dirección Nacional de Inteligencia - DINI y la resolución que emite el Vocal Superior Ad hoc, se tramitan dentro de las veinticuatro horas de presentada; en forma personal e indelegable.</p> <p>20.7 Ante resolución denegatoria del Vocal Superior Ad hoc, procede recurso de apelación ante la Sala que integra; la apelación se tramita y resuelve en el plazo de veinticuatro horas.</p>



Tabla 2, (continua) LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: CONTROL DE LA ACTIVIDAD DE INTELIGENCIA	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p>32.2 Su ejecución requiere autorización judicial otorgada por cualquiera de los dos (2) Jueces Superiores <i>ad hoc</i> del Poder Judicial, designados por la Corte Suprema de Justicia de la República, conforme al procedimiento señalado en el presente Decreto Legislativo. Todo el proceso constituye información clasificada como secreta.</p>	<p><b>Artículo 20.- Control judicial para operaciones especiales</b></p> <p>20.1 Para el control judicial de las operaciones especiales, la Corte Suprema de Justicia de la República designa dos Vocales Superiores Ad hoc.</p> <p>20.2 Las operaciones especiales requieren autorización judicial otorgada por cualquiera de los Vocales Superiores Ad hoc del Poder Judicial conforme al procedimiento señalado en la presente Ley. Todo el proceso constituye información clasificada como secreta.</p>
<p><b>Artículo 33.- Trámite</b></p> <p>33.1 La autorización para la ejecución de un procedimiento especial de obtención de información será solicitada únicamente por el Director de Inteligencia Nacional, y deberá contener lo siguiente:</p> <p>33.1.1 Identificación de la persona o personas que serán afectadas.</p> <p>33.1.2 Especificación de las medidas que se solicitan.</p> <p>33.1.3 Motivación y duración de las medidas solicitadas.</p>	<p>20.3 Las operaciones especiales son solicitadas debidamente motivadas por el Director Ejecutivo de la DINI a cualquiera de los dos Vocales Superiores Ad hoc del Poder Judicial.</p>
<p>33.2 La resolución judicial que emite el Juez Superior <i>ad hoc</i>, se tramita dentro de las veinticuatro (24) horas de presentada la solicitud del Director de Inteligencia Nacional, en forma personal e indelegable.</p>	

<b>Tabla 2, (continua)</b> <b>LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección:</b> <b>CONTROL DE LA ACTIVIDAD DE INTELIGENCIA</b>	
<b>Decreto Legislativo N° 1141 (vigente)</b>	<b>Ley N° 28664 (derogada)</b>
<p>33.4 Ante resolución denegatoria del Juez Superior <i>ad hoc</i>, procede recurso de apelación, el que será resuelto por una Sala Superior <i>ad hoc</i> presidida por el otro Juez Superior <i>ad hoc</i> y los dos Jueces Superiores <i>ad hoc</i> suplentes. De no constituirse dicha Sala, resolverá la que integra el Juez Superior <i>ad hoc</i> que no se pronunció. La apelación se tramita y resuelve en el plazo de veinticuatro (24) horas.</p>	
<p>33.5 En caso de peligro contra la seguridad nacional y por la urgencia de las circunstancias, el Director de Inteligencia Nacional podrá, excepcionalmente, autorizar la ejecución de un procedimiento especial de obtención de información, con cargo a formalizar la solicitud de inmediato ante el Juez Superior <i>ad hoc</i>, quien en plazo de veinticuatro (24) horas puede convalidarlo o disponer su inmediata paralización. Ante mandato de paralización, procede recurso de apelación.</p>	<p>20.4 En caso de peligro contra la seguridad nacional y por la urgencia de las circunstancias es necesario realizar una operación especial, el Director Ejecutivo de la DINI, puede excepcionalmente autorizarla con cargo a formalizar la solicitud de inmediato ante el Vocal Superior <i>Ad hoc</i>, quien en el plazo de veinticuatro horas puede convalidar o disponer la inmediata paralización de la operación especial; y en cumplimiento de la última parte del párrafo 21.2 comunica las razones y fundamentos de su decisión.</p>
<p><b>Artículo 34.- Valor probatorio de los informes de inteligencia</b>                      En ningún caso los informes de inteligencia tendrán valor probatorio dentro de procesos judiciales, administrativos y/o disciplinarios, pero su contenido podrá constituir elemento orientador durante la investigación. En ese caso, la autoridad correspondiente deberá observar lo dispuesto en el artículo 5° del presente Decreto Legislativo.</p>	

<b>Tabla 2, (continua)</b> <b>LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección:</b> <b>CONTROL DE LA ACTIVIDAD DE INTELIGENCIA</b>	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p><b>Artículo 35.- Destrucción de información innecesaria</b>                      Toda información obtenida para la producción de inteligencia por el SINA, que sea innecesaria para el objetivo del sistema por corresponder a los derechos fundamentales de la persona humana y a la esfera de su vida privada, debe ser destruida por los funcionarios responsables de los componentes del sistema que la detenten, bajo responsabilidad de inhabilitación y sin perjuicio de las sanciones civiles y/o penales que correspondan.</p>	
<p><b>CAPÍTULO II</b>  <b>CONTROL PARLAMENTARIO</b></p>	
<p><b>Artículo 36.- Control por la Comisión de Inteligencia del Congreso de la República y funciones</b>                      36.1 La Comisión de Inteligencia del Congreso de la República ejerce la fiscalización y control de las actividades del SINA.</p>	<p><b>Artículo 21.- Control por la Comisión de Inteligencia del Congreso de la República y funciones</b>                      21.1 La fiscalización de las actividades del SINA, por el Congreso de la República, es ejercida por la Comisión de Inteligencia, o la que haga sus veces.</p>
<p>36.2 La Comisión de Inteligencia puede requerir información clasificada y no clasificada a todos los componentes del SINA, por intermedio de la DINI, así como disponer investigaciones de oficio. Asimismo, puede requerir información clasificada a los Jueces Superiores <i>ad hoc</i>.</p>	<p>21.2 La Comisión de Inteligencia puede requerir información clasificada y no clasificada a todos los componentes del SINA, por intermedio de la DINI, e investigar de oficio. Asimismo puede requerir información clasificada a los Vocales Superiores Ad hoc.</p>

## Gestión de Inteligencia en las Américas

<b>Tabla 2, (continua)</b> <b>LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección:</b> <b>CONTROL DE LA ACTIVIDAD DE INTELIGENCIA</b>	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p>36.3 La Comisión de Inteligencia, además de las funciones que realiza como Comisión Ordinaria del Congreso de la República, está facultada para:</p> <p>36.3.1 Tomar conocimiento del Plan de Inteligencia Nacional - PIN, y [de] los Planes Institucionales de Inteligencia - PII, así como [de] las políticas que sobre la materia emitan el ente rector y los componentes del SINA.</p> <p>36.3.2 Solicitar un informe anual, con carácter secreto y por escrito, al ente rector del SINA, sobre las actividades de inteligencia programadas y ejecutadas por los componentes del SINA, de acuerdo al PIN.</p>	<p>21.3 Asimismo, la Comisión de Inteligencia está facultada para:</p> <p>a) Fiscalizar el Plan Anual de Inteligencia - PAI, así como las políticas que sobre la materia emitan los componentes del sistema y el Órgano Rector del SINA.</p> <p>b) Solicitar un Informe Anual con carácter secreto y por escrito al Director Ejecutivo de la DINI, sobre las actividades de inteligencia y contrainteligencia programadas y efectuadas.</p>
<p>36.4 El Director de Inteligencia Nacional remitirá un informe anual a la Comisión de Inteligencia del Congreso de la República, sobre su gestión en el logro de metas y objetivos alcanzados.</p>	
<p><b>Artículo 37.- Composición de la Comisión de Inteligencia del Congreso de la República</b></p> <p>37.1 La Comisión de Inteligencia del Congreso está integrada por no menos de cinco (5) ni más de siete (7) miembros permanentes elegidos por el Pleno del Congreso de la República, por todo el período parlamentario; respetando los criterios de pluralidad y especialidad; no pudiendo designarse miembros accesorios.</p>	<p><b>Artículo 22.- Composición de la Comisión de Inteligencia del Congreso de la República</b></p> <p>22.1 La Comisión de Inteligencia del Congreso está integrada por no menos de cinco (5) ni más de siete (7) miembros permanentes elegidos por el Pleno del Congreso de la República, por todo el período parlamentario; respetando los criterios de pluralidad y especialidad; no pudiendo designarse miembros accesorios.</p>

<b>Tabla 2, (continua)</b> <b>LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección:</b> <b>CONTROL DE LA ACTIVIDAD DE INTELIGENCIA</b>	
<b>Decreto Legislativo N° 1141 (vigente)</b>	<b>Ley N° 28664 (derogada)</b>
37.2 Los miembros titulares de la Comisión de Inteligencia eligen anualmente a su Presidente. La reelección inmediata está permitida.	22.2 Los miembros titulares de la Comisión de Inteligencia eligen anualmente a su Presidente. La reelección inmediata está permitida.
37.3 Los miembros de la Comisión de Inteligencia guardan secreto de la información clasificada de la que tomen conocimiento, aún después del término de sus funciones.	22.3 Los miembros de la Comisión de Inteligencia guardan secreto de la Información clasificada de la que tomen conocimiento, aun después del término de sus funciones.
37.4 Las sesiones de la Comisión de Inteligencia tienen carácter de secretas cuando la naturaleza de los temas a tratar lo ameriten; en dicho caso sólo participan sus miembros permanentes, y por acuerdo mayoritario de los mismos puede autorizarse la participación de alguno de sus pares.	22.4 Las sesiones de la Comisión de Inteligencia tienen carácter de secretas cuando la naturaleza de los temas a tratar lo ameriten; en dicho caso sólo participan sus miembros permanentes, y por acuerdo mayoritario de los mismos puede autorizarse la participación de alguno de sus pares.
<b>TÍTULO V</b> <b>MEDIDAS DE PROTECCIÓN DEL</b> <b>PERSONAL DE INTELIGENCIA</b> <b>Y DE LA ACTIVIDAD</b> <b>DE INTELIGENCIA</b>	
<b>Artículo 38.- Protección de la identidad</b>	
38.1 Los procedimientos de protección de identidad del personal y de la actividad de inteligencia, tienen carácter secreto.	
38.2 Los componentes del SINA podrán utilizar medios y realizar actividades encubiertas, que resulten necesarios para garantizar la seguridad del personal de inteligencia y el cumplimiento de los objetivos del SINA en materia de seguridad nacional. Corresponde a la DINI dictar las normas y procedimientos para este fin.	

## Gestión de Inteligencia en las Américas

<b>Tabla 2, (continua)</b> <b>LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección:</b> <b>CONTROL DE LA ACTIVIDAD DE INTELIGENCIA</b>	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p>38.3 Las autoridades y entidades competentes, se encuentran obligadas a expedir los documentos de identidad, matrículas, licencias, permisos y otros que resulten necesarios para garantizar las actividades mencionadas en el numeral anterior.</p>	
<p><b>Artículo 39.- Responsabilidades</b></p> <p>39.1 Los documentos expedidos de acuerdo a lo regulado en la presente Ley, podrán ser utilizados para el trámite de documentos públicos y privados, entre otros, estrictamente necesarios para el cumplimiento de los objetivos de la actividad de inteligencia, sin que ello genere responsabilidades administrativas, civiles o penales.</p>	
<p>39.2 En caso de investigación por el uso de los documentos a que se refiere el artículo 38° de la presente Ley, basta la presentación de un informe del director o jefe del componente respectivo justificando su empleo, para el archivo definitivo de dicha investigación en toda instancia.</p>	
<p>39.3 El reglamento establecerá las causales de caducidad de los documentos expedidos en el marco del presente Decreto Legislativo.</p>	
<p><b>Artículo 40.- De la reserva de información</b></p> <p>El personal de las entidades públicas que expida documentos, matrículas, licencias, permisos y otros, en virtud de lo normado en la presente norma, está obligado a guardar reserva de la información, así como mantener el carácter</p>	

<b>Tabla 2, (continua)</b> <b>LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección:</b> <b>CONTROL DE LA ACTIVIDAD DE INTELIGENCIA</b>	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p>clasificado de su existencia y contenido, en el marco de lo dispuesto por el artículo 4° del presente Decreto Legislativo.</p>	
<p><b>Artículo 41.- Protección del núcleo familiar</b>                      Los titulares de los sectores a los que pertenecen los componentes del SINA, garantizan mediante los mecanismos que establece el reglamento de la presente ley, la seguridad e integridad del personal de inteligencia y de su núcleo familiar frente a peligro inminente de su vida a consecuencia del desarrollo de actividades de inteligencia.</p>	
<p><b>TÍTULO VI</b>  <b>OBLIGACIÓN DE INFORMAR</b>  <b>DE ENTIDADES PÚBLICAS</b>  <b>Y PRIVADAS</b></p>	
<p><b>Artículo 42.- Obligación de informar</b>                      42.1 Los titulares, funcionarios y personal, de todas las instituciones conformantes de la administración pública, contribuyen con el SINA, brindando obligatoriamente la información que le sea requerida por el ente rector del sistema.</p>	<p><b>Artículo 12.- Obligación de informar</b>                      12.1 Los titulares, funcionarios y personal, de todas las instituciones conformantes de la administración pública, contribuyen con el SINA, brindando obligatoriamente la información pertinente a los objetivos del Sistema.</p>
<p>42.2 Toda persona natural o jurídica contribuye con el SINA, brindando obligatoriamente y en forma gratuita, la información que sea requerida por el ente rector del sistema, vinculada a las labores de inteligencia.</p>	
<p>42.3 En caso que la información solicitada esté amparada por algún deber de reserva, la entrega de tal información no constituirá una violación a dicho deber,</p>	

## Gestión de Inteligencia en las Américas

<b>Tabla 2, (continua)</b> <b>LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección:</b> <b>CONTROL DE LA ACTIVIDAD DE INTELIGENCIA</b>	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p>toda vez que la misma continuará bajo este principio, al cual se encuentra obligado todo el personal de inteligencia en virtud de lo dispuesto en el presente Decreto Legislativo.</p>	
<p>42.4 Todo el procedimiento constituye información clasificada como secreta.</p>	
<p>42.5 Están exceptuados de los alcances de este artículo, las informaciones protegidas por el secreto profesional, intimidad personal y familiar, secreto bancario, reserva tributaria y otras que la Constitución Política ampare.</p>	
<p>42.6 El cumplimiento de la obligación de informar dispuesto en el presente artículo, no requiere ser complementado con la suscripción de ningún convenio o acuerdo, bastando únicamente el propio mandato legal. El incumplimiento de esta disposición acarrea responsabilidad.</p>	
	<p>12.2 La UIF sólo está obligada a brindar información a la DINI, cuando corresponda comunicar al Ministerio Público, siempre que lo comunicado contenga información que pueda atentar contra la seguridad nacional.</p> <p>12.3 La comunicación de la UIF se cursa simultáneamente al Ministerio Público y a la DINI.</p>
<p><b>Artículo 43.- Obligación de informar a la Unidad de Inteligencia Financiera del Perú</b>                      La DINI sólo está obligada a brindar información a la Unidad de Inteligencia Financiera del Perú, relativa a</p>	<p>12.4 La DINI sólo está obligada a brindar Información a la UIF, relativa a lavado de activos y/o financiamiento de terrorismo.</p>



<b>Tabla 2, (continua)</b> <b>LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección:</b> <b>CONTROL DE LA ACTIVIDAD DE INTELIGENCIA</b>	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
lavado de activos y/o financiamiento de terrorismo.	
<p style="text-align: center;"><b>DISPOSICIONES COMPLEMENTARIAS FINALES</b></p> <p><b>PRIMERA.- Financiamiento</b>                      Lo dispuesto en el presente Decreto Legislativo se financia con cargo al presupuesto institucional de la DINI, sin demandar recursos adicionales al Tesoro Público.</p> <p><b>SEGUNDA.- Aprobación del Reglamento</b>                      El reglamento del presente Decreto Legislativo será aprobado en un plazo no mayor a noventa (90) días calendario contados desde la publicación del presente en el Diario Oficial El Peruano.</p> <p><b>TERCERA.- Aprobación del Reglamento de Organización y Funciones de la DINI</b>                      El Reglamento de Organización y Funciones (ROF) de la DINI se presentará en el plazo máximo de sesenta (60) días calendarios contados a partir de la vigencia del presente Decreto Legislativo, para su aprobación en el Consejo de Ministros de conformidad con la normativa aplicable.</p> <p><b>CUARTA.- Recursos humanos</b>                      El Cuadro para Asignación de Personal (CAP) y el Presupuesto Analítico de Personal (PAP) de la DINI se presentarán en el plazo máximo de ciento veinte (120) días calendario, respectivamente, de aprobado el Reglamento de</p>	

## Gestión de Inteligencia en las Américas

Tabla 2, (continua) LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: CONTROL DE LA ACTIVIDAD DE INTELIGENCIA	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p>Organización y Funciones (ROF), de acuerdo con la normatividad aplicable.</p> <p><b>QUINTA.- Escala remunerativa de la DINI</b>                      Exonérese a la Dirección Nacional de Inteligencia -DINI de lo establecido en el artículo 6° de la Ley N° 29951, Ley de Presupuesto del Sector Público para el Año Fiscal 2013, para la aprobación de su escala remunerativa.</p> <p>Dicha escala se aprueba conforme a lo establecido en la Cuarta Disposición Transitoria de la Ley N° 28411, Ley General del Sistema Nacional de Presupuesto, previo informe favorable de la Dirección General de Presupuesto Público, y de la Dirección General de Gestión de Recursos Públicos del Ministerio de Economía y Finanzas.</p> <p>La presente disposición rige a partir del 2 de enero de 2013, quedando en suspenso y/o sin efecto, según corresponda, las normas que se le opongan.</p> <p><b>SEXTA.- Capacitación para el personal de la administración pública</b>                      La DINI ejecuta programas de capacitación para los Jueces Superiores Ad hoc del Poder Judicial designados para autorizar los procedimientos especiales de obtención de información; para la Comisión de Inteligencia del Congreso de la República; para el personal de la Contraloría General de la República que realiza las auditorías; para el personal del Registro Nacional de Identificación de</p>	

Tabla 2, (continua) LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección: CONTROL DE LA ACTIVIDAD DE INTELIGENCIA	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p>inteligencia y contrainteligencia, de acuerdo a las necesidades del SINA y de la DINI.</p> <p><b>SÉPTIMA.- Conservación de clasificación</b>                      Las informaciones clasificadas de acuerdo al régimen establecido por la Ley 28664, y la Ley de Transparencia y Acceso a la Información Pública, continuarán conservando su clasificación por el tiempo señalado en dichas normas.</p> <p style="text-align: center;"><b>DISPOSICIONES COMPLEMENTARIAS TRANSITORIAS</b></p> <p><b>PRIMERA.- Nombramiento del primer Director de Inteligencia Nacional y Director Ejecutivo de la DINI</b>                      El Presidente de la República nombra al primer Director de Inteligencia Nacional y al Director Ejecutivo de la DINI, dentro de los treinta (30) días siguientes a la publicación del presente Decreto Legislativo.</p> <p><b>SEGUNDA.- Personal temporal de otras entidades</b>                      Las Fuerzas Armadas y la Policía Nacional del Perú podrán asignar temporalmente y en forma proporcional personal militar y policial calificado, de acuerdo al perfil requerido por la DINI para el cumplimiento de sus funciones. Para dicho efecto, este personal tendrá derecho a la Bonificación por Alto Riesgo a la Vida prevista en el literal c) del artículo 8 del Decreto Legislativo N° 1132, Decreto Legislativo que aprueba la nueva Estructura de Ingresos aplicable al</p>	

## Gestión de Inteligencia en las Américas

<b>Tabla 2, (continua)</b> <b>LEGISLACIÓN DE INTELIGENCIA EN PERÚ / Sección:</b> <b>CONTROL DE LA ACTIVIDAD DE INTELIGENCIA</b>	
Decreto Legislativo N° 1141 (vigente)	Ley N° 28664 (derogada)
<p>personal militar de las Fuerzas Armadas y policial de la Policía Nacional del Perú, cuyo pago será por cuenta del pliego de origen. Las normas reglamentarias del citado Decreto Legislativo establecen las condiciones del otorgamiento de la bonificación mencionada.</p> <p><b>TERCERA.- Recursos especiales</b></p> <p>Precítese que los instrumentos y normativa interna que regulan la autorización, ejecución, sustentación y control de la rendición de cuentas de los recursos especiales utilizados por el SINA, continuarán siendo de plena aplicación hasta la aprobación de la directiva a la que se refiere el artículo 30° del presente Decreto Legislativo.</p> <p style="text-align: center;"><b>DISPOSICIONES COMPLEMENTARIAS DEROGATORIAS</b></p> <p><b>PRIMERA.- Norma derogatoria</b></p> <p>Deróguense la Ley 28664. Ley del SINA y de la DINI; así como las demás normas que se opongan al presente Decreto Legislativo.</p> <p><b>SEGUNDA.- Vigencia</b></p> <p>El presente Decreto Legislativo entra en vigencia al día siguiente de su publicación en el Diario Oficial El Peruano.</p>	

**Fuente:** Andrés Gómez de la Torre Rotta.

## Biografías de los autores

**Andrés Gómez de la Torre Rotta.** Peruano. Abogado. Maestría en Política y Economía Internacional (Universidad de Belgrano, Buenos Aires). Egresado del CHDS-Washington. Cursos de postgrado en España (Ciencia Política, Derecho Internacional). Ex Director Nacional de Inteligencia Exterior - CNI (2001), ex asesor parlamentario en la Comisión de Defensa Nacional, Orden Interno, Inteligencia, Desarrollo Alternativo y Lucha contra las Drogas y en Comisiones Investigadoras del Congreso de la República del Perú (2002-2007). Ex Director de la Escuela Nacional de Inteligencia - ENI (2007-2009) y docente en la misma (2007-2011). Miembro Asociado del Instituto de Estudios Internacionales (IDEI - Pontificia Universidad Católica del Perú). Ha participado como conferencista en eventos sobre paz, seguridad, defensa e inteligencia entre los años 2009, 2010 y 2011, llevados a cabo en Quito (FLACSO), Brasilia (Asociación Brasileira de Estudios de Defensa - ABED) y Rio de Janeiro (Agencia de Cooperación Social - Brasil & SIPRI-Suecia). Miembro de la Task Force - Grupo Perú, Programa de Cooperación de la Seguridad Regional, Fundación Friedrich Ebert. Coautor de la obra colectiva: *Inteligencia estratégica y Prospectiva*, publicada por FLACSO-Ecuador, Secretaría Nacional de Inteligencia (SENAIN) y AECI-España (2011). Coautor de la reciente obra colectiva: *Cuestiones de Inteligencia en la Sociedad Contemporánea*, editada por el Ministerio de Defensa de España, Centro Nacional de Inteligencia (CNI) y la Universidad Santiago de Compostela (2012). Correo: [Andres\\_gotorer@yahoo.es](mailto:Andres_gotorer@yahoo.es).

**Arturo Medrano Carmona.** Peruano. Licenciado en Ciencia Política y Asistente para la presente investigación. Estudió en la Escuela de Ciencia Política de la Universidad Nacional Federico Villarreal. Egresado del Centro de Altos Estudios Nacionales (CAEN). Participó en el III Juego Estratégico Computarizado *Nation Lab*, organizado por el Comando Sur de los Estados Unidos de Norteamérica – CAEN (2004). Especialista en Derecho Administrativo y Procedimientos Administrativos, Colegio de Abogados de Lima (CAL).

Gestión de Inteligencia en las Américas

Leyes de Inteligencia de Norteamérica,  
América Central y Sudamérica

Liza Zéniga Collado

Tabla 3  
Leyes de Inteligencia de Norteamérica, América Central y Sudamérica

1. País con ley y sistema de inteligencia			
País	Ley	Definición de inteligencia según la ley	Organismos principales
Argentina	Ley 25520 promulgada el 3/12/2001. Ley de Inteligencia Nacional, reemplazada por Ley 27126, 8 junio 2015, Agencia Federal de Inteligencia.	Inteligencia Nacional - la actividad consistente en la obtención, reunión, sistematización y análisis de la información específica referida a los hechos, riesgos y conflictos que afecten la Defensa Nacional y la seguridad interior de la Nación interior de la Nación (Ley 25250, Art.1)	a) Agencia Federal de Inteligencia. b) Dirección Nacional de Inteligencia Criminal, dependiente del Ministerio de Seguridad Pública. c) Dirección Nacional de Inteligencia Estratégica Militar, dependiente el Ministerio de Defensa.
Brasil	a) Ley 9883 del 7/12/1999. Instituye el sistema brasileño de inteligencia, crea la Agencia Brasileña de Inteligencia.	Actividad que tiene como fin la obtención, análisis y disseminación de conocimientos dentro y fuera del territorio nacional sobre hechos y situaciones de inmediata o potencial influencia sobre el proceso de acción y decisión gubernamental y sobre la salvaguardia y seguridad de la sociedad y del Estado (Ley 9833, Art. 1, Num. 2)	a) Agencia Brasileña de Inteligencia (ABIN) como órgano central, dependiente de Presidencia. b) Sistema Brasileño de Inteligencia, compuesto por 9 ministerios (a través de distintos órganos), más la Contraloría, la ABIN, el Centro gestor y operacional del Sistema de Protección de la Amazonia y el Gabinete de Seguridad Institucional de la Presidencia.

Tabla 3 , (continua)  
Leyes de Inteligencia de Norteamérica, América Central y Sudamérica

1. País con ley y sistema de inteligencia			
País	Ley	Definición de inteligencia según la ley	Organismos principales
Brasil	<p>b) Decreto N° 3695, del 21/12/ 2000. Crea el Subsistema de Inteligencia de Seguridad Pública.</p> <p>c) Decreto N° 4376 del 13/09/2002. Dispone la organización y funcionamiento del sistema brasileño de inteligencia.</p>		<p>c) Subsistema de Inteligencia de Seguridad Pública integrado por los Ministros de Justicia, Hacienda, Defensa e Integración Nacional, y el Gabinete de Seguridad Institucional de la Presidencia.</p>



Tabla 3 , (continua)  
Leyes de Inteligencia de Norteamérica, América Central y Sudamérica

1. País con ley y sistema de inteligencia		Organismos principales
País	Ley	Definición de inteligencia según la ley
Canadá	CSIS Act, 1984.	Inteligencia de seguridad es información formulada para ayudar a los del gobierno que toman decisiones y crean las políticas del Estado. Sin importar la fuente, esta información provee algo de valor mas allá de la que sea encontrada en informes de otras partes del gobierno o en las noticias diarias.
Chile	Ley sobre el sistema de inteligencia del Estado y creación de la Agencia Nacional de Inteligencia, ley 19974 promulgada el 27/09/2004	<p>a) Agencia Nacional de Inteligencia; como órgano central dependiente del Ministerio del Interior y Seguridad Pública.</p> <p>b) Dirección de Inteligencia de Defensa del Estado Mayor de la Defensa Nacional.</p> <p>c) Direcciones de Inteligencia de las Fuerzas Armadas.</p>

Tabla 3 , (continua)  
Leyes de Inteligencia de Norteamérica, América Central y Sudamérica

1. País con ley y sistema de inteligencia			
País	Ley	Definición de inteligencia según la ley	Organismos principales
Chile			d) Las Direcciones o Jefaturas de Inteligencia de las Fuerzas de Orden y Seguridad Pública.
Colombia	Ley N° 1621, vigente desde 17/04/2013.	La función de inteligencia y contrainteligencia es aquella que desarrollan los organismos especializados del Estado del orden nacional, utilizando medios humanos o técnicos para la recolección, procesamiento, análisis y difusión de información, con el objetivo de proteger los derechos humanos, prevenir y combatir amenazas internas o externas contra la convivencia democrática, la seguridad y la defensa nacional, y cumplir los demás fines enunciados en esta Ley. (Ley 1621, Art.2)	La Junta de Inteligencia Conjunta (JIC) es la que producirá estimativos de inteligencia y contrainteligencia para el Gobierno Nacional. Esta Junta está conformada por: a. El Ministro de la Defensa Nacional. b. El Alto Asesor para la Seguridad Nacional. c. El Viceministro de Defensa Nacional. d. El Jefe de Inteligencia Conjunta, en representación del Comandante General de las Fuerzas Militares. e. El Jefe de Inteligencia del Ejército Nacional, en representación del Comandante de esa Fuerza.

Tabla 3 , (continua)  
Leyes de Inteligencia de Norteamérica, América Central y Sudamérica

1. País con ley y sistema de inteligencia			
País	Ley	Definición de inteligencia según la ley	Organismos principales
Ecuador	Decreto Ejecutivo N° 1768 del 08/06/2009, crea la Secretaría de Inteligencia Ley de Seguridad Pública y del Estado 29/09/2009.	La actividad consistente en la obtención, sistematización y análisis de la información específica referida a las amenazas, riesgos y conflictos que afecten a la seguridad integral. La información de inteligencia es sustancial para la toma de decisiones en material de seguridad. (Art. 14 de la ley)	La Secretaría de Inteligencia es el órgano rector del Sistema Nacional de Inteligencia que está compuesto por: a) Subsistema de Inteligencia Militar, para la defensa nacional. b) Subsistema de Inteligencia Policial, para la protección interna. c) Unidad de Gestión de Seguridad Interna de la Presidencia de la República. d) Otros organismos de inteligencia que se crearen o adscribieren en el futuro. e) Otras instituciones y organismos que posean o produzcan información de interés para los fines de la conducción y seguridad integral del Estado.

Tabla 3 , (continua)  
Leyes de Inteligencia de Norteamérica, América Central y Sudamérica

1. País con ley y sistema de inteligencia			
País	Ley	Definición de inteligencia según la ley	Organismos principales
Estados Unidos	The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Ley Pública 108-485. Decreto Ejecutivo 12333, 1981; Decreto Ejecutivo 13355, 2004; y Decreto Ejecutivo 13470, 2008.	La inteligencia nacional es información recolectada desde dentro o afuera de los Estados Unidos que: A) consistente con la dirección del Presidente, tiene que ver con más de una agencia del gobierno; y B) trata con amenazas a los Estados Unidos, sus pueblos, bienes, o intereses; también el desarrollo, proliferación, o uso de armas de destrucción masiva; o cualquier asunto atinente a la seguridad nacional o de la patria.	Consejo de Seguridad Nacional, Director de Inteligencia Nacional, Centro Nacional de Contraterrorismo, Centro Nacional de Contraproliferación. Organismos de la Comunidad de Inteligencia: Agencia Central de Inteligencia, Agencia de Inteligencia de Defensa, Agencia de Seguridad Nacional, Oficina de Reconocimiento Nacional, Agencia de Inteligencia Geo-Espacial Nacional, Departamento de Estado (INR), Departamento de Seguridad de la Patria, Departamento (Ministro) de Hacienda, Departamento de Energía, Buró Federal de Investigaciones, Agencia Antidrogas, Servicios de Inteligencia del Ejército, la Armada, la Fuerza Aérea, la Infantería de Marina y el Guardacostas.

Tabla 3 , (continua)  
Leyes de Inteligencia de Norteamérica, América Central y Sudamérica

1. País con ley y sistema de inteligencia		
País	Ley	Definición de inteligencia según la ley
Guatemala	Decreto nº 71 de 2005. Ley de la Dirección General de la Inteligencia Civil y Decreto No.18-2008. Ley Marco del Sistema Nacional de Seguridad.	Si bien no se entrega una definición como tal, se señala que la DIGICL, tiene entre sus funciones “planear, recolectar y obtener información, procesarla, sistematizarla y analizarla, transformándola en inteligencia”. (Decreto 71-2005, Art. 3)
		Organismos principales Sistema de Inteligencia Nacional forma parte del Sistema Nacional de Seguridad y se compone de: 1) Secretaría de Inteligencia Estratégica. 2) Dirección de Inteligencia Civil del Ministerio de Gobernación. 3) Dirección de Inteligencia del Estado Mayor de la Defensa Nacional del Ministerio de la Defensa Nacional.

Tabla 3, (continua)  
Leyes de Inteligencia de Norteamérica, América Central y Sudamérica

1. País con ley y sistema de inteligencia		Definición de inteligencia según la ley	Organismos principales
País	Ley		
Honduras	Decreto Legislativo 211-2012, 15/04/2013 abril 2013, crea la Dirección Nacional de Investigación e Inteligencia (DNIE), como organismo independiente, nominalmente civil, dependencia del Consejo Nacional de Seguridad y Defensa. Se crea también un Sistema Nacional de Inteligencia, junto con un Comité de Inteligencia Estratégica.	La DNIE, tendrá como objeto desarrollar actividades de investigación e inteligencia estratégica para proteger los derechos y libertades de los ciudadanos y residentes en el país, prevenir y contrarrestar amenazas internas o externas contra el orden constitucional y ejecutar las políticas públicas que en materia de defensa y seguridad establezca el Consejo Nacional de Defensa y Seguridad.	La DNIE coordina el Sistema Nacional de Inteligencia y preside su Comité de Inteligencia Estratégica. Miembros del sistema son: a) Fuerzas Armadas; b) Policía Nacional; c) Secretaría de Estado en el Despacho de Relaciones Exteriores; d) Unidad de Información Financiera.
Perú	Decreto Legislativo 1141, del 11/12/2012. Ley 28664 del 2006.	Actividad que comprende un proceso sistemático de búsqueda, evaluación y análisis de información, cuya finalidad es producir conocimiento útil para la toma de decisiones. (Decreto Legislativo 1141, Art. 2)	Sistema de Inteligencia Nacional (SINA), forma parte del Sistema de Seguridad Nacional y se compone de: a) Consejo de Inteligencia Nacional. b) Dirección Nacional de Inteligencia.

Tabla 3 , (continua)  
Leyes de Inteligencia de Norteamérica, América Central y Sudamérica

1. País con ley y sistema de inteligencia			
País	Ley	Definición de inteligencia según la ley	Organismos principales
Uruguay	Se debate en el congreso una ley nacional de inteligencia.* Es anticipada que la ley creará una Secretaría de Inteligencia Estratégica de Estado, dependiente de la Presidencia de la República.	La actividad de inteligencia se desarrollará bajo los principios de protección y defensa de los intereses estratégicos nacionales.	<p>c) Dirección General de Asuntos Multilaterales y Globales del Ministerio de Relaciones Exteriores.</p> <p>d) Defensa: Segunda División de Estado Mayor del Comando Conjunto de las FF.AA.; Dirección de Inteligencia de las FF.AA., respectivamente.</p> <p>e) Interior: Dirección General de Inteligencia del Ministerio del Interior (DIGIMIN) y Dirección de Inteligencia de la Policía Nacional (DIRIN).</p> <p>El Sistema Nacional de Inteligencia estará integrado por una Secretaría de Inteligencia del Estado, junto con organismos de los ministerios de Defensa Nacional, Interior, Relaciones Exteriores, y Economía.</p>

Tabla 3 , (continua)  
Leyes de Inteligencia de Norteamérica, América Central y Sudamérica

2. Países con ley de agencias centralizadoras de información			
País	Ley	Función del organismo civil de inteligencia	Organismos
Costa Rica	Ley nº 7410 del 26/05/1994-Ley general de policía, y Decreto ejecutivo 23758 de 1994, sobre Dirección de Inteligencia y Seguridad Nacional.	La Dirección de Inteligencia y Seguridad Nacional realizará operaciones de inteligencia que permitan recopilar y posteriormente verificar la información necesaria.	Departamento de Inteligencia Policial, de la Fuerza pública. Dirección de Inteligencia y Seguridad Nacional.
El Salvador	Decreto nº 554 del 20/09/2001. Ley del Organismo de Inteligencia del Estado	Se señala que la función del organismo es "informar y asesorar al Presidente de la República en materia de inteligencia, lo necesario para la satisfacción de los objetivos nacionales vinculados al desarrollo del país, la seguridad del Estado y la vigencia del régimen democrático, referida especialmente a todos los campos de la seguridad nacional" (Decreto 554, Art. 5)	Organismo de Inteligencia del Estado, dependiente de Presidencia. Centro de Inteligencia Policial de la Policía Nacional Civil. Dirección de Inteligencia del Estado Mayor de la Fuerza Armada.
México	Ley de Seguridad Nacional, 2005.	CISEN tiene el propósito de generar inteligencia estratégica, táctica	El Centro de Investigación y Seguridad Nacional (CISEN) es un órgano de inteligencia



<p>Tabla 3, (continua) Leyes de Inteligencia de Norteamérica, América Central y Sudamérica</p>			
<p>2. Países con ley de agencias centralizadoras de información</p>			
País	Ley	Función del organismo civil de inteligencia	Organismos
México, continua		y operativa que permita preservar la integridad, estabilidad y permanencia del Estado Mexicano, dar sustento a la gobernabilidad y fortalecer al Estado de Derecho. Su papel es alertar y proponer medidas de prevención, disuasión, contención y neutralización de riesgos y amenazas que pretendan vulnerar el territorio, la soberanía, al orden constitucional, las libertades e instituciones democráticas de los mexicanos, así como el desarrollo económico, social y político del país.	civil dependiente de la Oficina del Presidente. La Policía Federal, el Ejército, la Armada y la Fuerza Aérea cuentan con oficinas de inteligencia.
Panamá	Ley no. 15, 14 abril 2010, crea el Ministerio de Seguridad Pública. (Ley no. 8 de 2008 fue abrogada en 2010)	Ninguna	A ser determinado por Ministerio de Seguridad Pública

Tabla 3, (continua)  
Leyes de Inteligencia de Norteamérica, América Central y Sudamérica

2. Países con ley de agencias centralizadoras de información			
País	Ley	Función del organismo civil de inteligencia	Organismos
Paraguay	Ley 5241, crea el Sistema Nacional de Inteligencia (SINAI), 21 agosto 2014	Crear conocimiento útil para presentarlos a disposición del Presidente de la República y a los diversos niveles superiores de conducción del Estado, para garantizar la paz y seguridad del Estado, proteger la soberanía nacional, preservar el orden constitucional y el régimen democrático vigente.	Dirección de Inteligencia Estratégica del Ministerio de Defensa Nacional y de Fuerzas Armadas; Ministerio del Interior; Policía Nacional, Secretaría Nacional Antidrogas; Análisis Financiero

Tabla 3, (continua)  
Leyes de Inteligencia de Norteamérica, América Central y Sudamérica

2. Países con ley de agencias centralizadoras de información			
País	Ley	Función del organismo civil de inteligencia	Organismos
Venezuela	Decreto 6865, 11 agosto 2009; Decreto 8792, 31 enero 2012; otros pendientes para dar clarificación a ley de inteligencia, Decreto 6068, de 14 mayo 2008.	El SEBIN tendrá por objeto planificar, formular, dirigir, controlar y ejecutar políticas y acciones de inteligencia y contrainteligencia de carácter civil y sus actuaciones estarán fundamentadas en los principios de honestidad, participación, celeridad, eficacia, eficiencia, transparencia, responsabilidad social, preeminencia al respecto de los derechos humanos, la ética, el pluralismo político y sometimiento pleno a la ley. (Decreto 7.453, Artículo 2)	Servicio Bolivariano de Inteligencia Nacional (SEBIN), depende del Ministerio de Poder Popular para Relaciones Interiores y Justicia. Ramas de inteligencia de las Fuerzas Armadas Bolivarianas conjuntas, dependientes del Poder Popular para la Defensa en el ámbito militar.

Tabla 3.

Fuente: Liza Zúñiga, con adiciones por los editores.

\* La fuente para los detalles aquí presentados es un informe de un periódico uruguayo, "Actividad de Inteligencia estará regulada por ley", de 4 junio 2013, disponible en <http://www.republica.com.uy/estara-regulada-por-ley/>.

## Guardando os Guardiães: O Controle dos Serviços Secretos no Regime Democrático

Joanisval Brito Gonçalves

*When oversight has been capable and constructive, it has been a major asset to the IC [Intelligence Community]. When degraded or misused, it has been an albatross around the neck of the intelligence agencies.*

—Marvin Ott

*International Journal of Intelligence and CounterIntelligence* (Winter 2003)

### Introdução

Nas democracias modernas, a atividade de inteligência é imprescindível para fazer frente às ameaças ao Estado e à sociedade e também para a identificação de oportunidades em diferentes áreas. Afinal, o Estado e a sociedade precisam ser protegidos, e os tomadores de decisão nas mais altas esferas da Administração pública necessitam de assessoramento nos moldes do realizado pelos serviços secretos.

Entretanto, convém destacar que a atividade de Inteligência não é uma atividade habitual do Estado Democrático. Segundo José Manuel Ugarte, “é uma atividade, se bem que permanente, excepcional de referido Estado, reservada para o exterior, das questões mais importantes das políticas exterior, econômica e de defesa; e para o interior, àquelas ameaças susceptíveis de destruir o Estado e o sistema democrático”.<sup>133</sup> Tem-se aí o grande dilema sobre o papel da inteligência em regimes democráticos: como conciliar a tensão entre a necessidade premente do segredo (sigilo) na atividade de inteligência e a transparência das atividades estatais, essencial em uma democracia?

Ademais, outra preocupação surge, particularmente nas sociedades democráticas que viveram períodos autoritários em passado recente (a exemplo de países da América Latina e do Leste Europeu): como garantir que os órgãos de segurança e inteligência desenvolvam suas atividades de maneira consentânea com os princípios democráticos, evitando abusos e arbitrariedades contra

essa ordem democrática e contra os direitos e garantias fundamentais dos cidadãos?<sup>134</sup>

A maneira com que determinada sociedade lida com o dilema transparência *versus* sigilo, em termos de procedimentos e atribuições dos serviços de inteligência, é um indicador do grau de desenvolvimento da democracia nessa sociedade.<sup>135</sup> Em democracias consolidadas, a dicotomia transparência das ações governamentais *versus* sigilo da atividade de inteligência é resolvida, por definição, com o uso de mecanismos eficientes e efetivos de fiscalização e controle interno e, especialmente, de controle externo, exercido primordialmente pelo Poder Legislativo.

O presente ensaio tem por objetivo discorrer sobre as relações entre a atividade de inteligência desenvolvida em regimes democráticos e seus mecanismos de controle. Nesse sentido, pretende-se apresentar os aspectos básicos sobre fiscalização e controle no campo da inteligência e os mecanismos por meio dos quais os serviços secretos podem ser controlados em uma democracia. Conclui-se com algumas orientações e práticas que podem ser úteis no estabelecimento de um arcabouço normativo e institucional para o controle dos serviços secretos. Preliminarmente, porém, é conveniente que seja feita breve apresentação sobre a atividade de inteligência em si, também chamada por alguns de “o ofício do espião”.

### Inteligência e democracia

Embora tão antiga quanto a existência humana, a atividade de inteligência é pouco conhecida fora do seletor grupo de iniciados que a operam. Nesse sentido, o desconhecimento contribui para que permaneça a tensão entre o sigilo necessário e a transparência desejável quando se lida com o tema, em especial no que concerne à maneira como a opinião pública percebe os serviços secretos e suas atividades.<sup>136</sup>

Importante destacar que inteligência se divide, para fins didáticos e algumas vezes operacionais, em três funções, missões ou ramos: inteligência (relacionada à reunião e análise de informações para produção de conhecimento); contra-inteligência (que objetiva proteger seu próprio conhecimento e neutralizar a inteligência adversa); e operações de inteligência (compreendidas como as ações, inclusive com recurso a meios e técnicas sigilosos e intrusivos,

## Gestão de Inteligência em las Américas

para a obtenção dos dados protegidos).<sup>137</sup>

Definida inteligência e sabendo-se que ela pode ser útil no assessoramento ao processo decisório, cabe uma constatação: a de que a atividade de inteligência não é “boa nem má”, mas sim um instrumento de grande relevância em qualquer regime político. E isso se deve ao fato de que os serviços secretos lidam eminentemente com informação, e informação (conhecimento) é poder. Logo, um dirigente habilidoso consegue conduzir melhor suas atividades se souber utilizar adequadamente o setor de inteligência.<sup>138</sup> E, quando isso acontece, seja em democracias, seja em regimes autoritários, os serviços secretos podem-se tornar, eles próprios, tremendamente poderosos.

Destaque-se que, por lidarem com muito poder, os serviços de segurança e inteligência podem extrapolar suas funções e cometer arbitrariedades, inclusive contra o Estado e a sociedade que teriam por missão proteger.

### O controle da atividade de inteligência – aspectos gerais<sup>139</sup>

Um dos fundamentos do regime democrático é o controle popular (direto ou indireto) que deve ser exercido sobre as instituições e agentes estatais. Hely Lopes Meirelles associa regimes democráticos a mecanismos eficientes e eficazes de controle sobre o Poder Público e a Administração Pública.<sup>140</sup>

Segundo Meirelles, o controle da Administração pública é a faculdade de vigilância, orientação e “correção que um Poder, órgão ou autoridade exerce sobre a conduta funcional de outro”.<sup>141</sup> Utiliza-se a terminologia “controle interno” para aquele exercido por órgãos da própria Administração (como a Corregedoria-Geral da União, no sistema administrativo brasileiro, ou o *Auditor-General* ou *Inspector-General*, em modelos anglo-saxônicos), ou seja, integrantes do Poder Executivo. Já o “controle externo” é o efetuado por órgãos alheios à Administração,<sup>142</sup> vinculados geralmente aos Poderes Legislativo e Judiciário. Há, ainda, o controle externo popular, relacionado ao direito individual do cidadão ou coletivo da sociedade de fiscalizar as ações do Estado.<sup>143</sup>

Alguns esclarecimentos terminológicos: de acordo com a perspectiva anglo-saxônica, controle (*control*) e fiscalização (*oversight*) estariam em patamares distintos. Enquanto *control* refere-se aos atos quotidianos de gerenciamento

da Administração, sendo de responsabilidade primordial do Poder Executivo, *oversight* estaria ligado às atribuições do poder legislativo de fiscalizar se o executivo (ou seja, a Administração pública) tem-se conduzido de acordo com princípios legais e constitucionais.<sup>144</sup> O termo *control* sob a ótica anglo-saxônica poderia ser mais bem traduzido como “supervisão”.

De toda maneira, tanto em termos de *control* quanto de *oversight* está presente a idéia de *accountability*, termo que em português relaciona-se à “prestação de contas”, em sentido amplo, inerente à atividade pública: “*Accountability is an information process whereby an agency is under a legal obligation to answer truly and completely the questions put it by an authority to which it is accountable (for example, a parliamentary intelligence oversight committee)*”.<sup>145</sup> Destaque-se, nesse sentido, que em língua portuguesa não existe tradução para a palavra *accountability*. Essa é uma particularidade que poderia ser associada à maneira como tradicionalmente a sociedade brasileira lida com a gestão da coisa pública.<sup>146</sup>

Logo, enquanto o controle envolve um conjunto de parâmetros e limitações legais aos quais se deve ater a Administração, a fiscalização refere-se ao legítimo poder de determinadas instituições e autoridades de averiguar o cumprimento das atribuições da Administração pública em conformidade com o arcabouço jurídico-normativo, aí incluídos os princípios que regem essa Administração.<sup>147</sup> Já *accountability* diz respeito ao dever dos agentes públicos de prestar contas sobre seus atos<sup>148</sup> e ao dever daqueles com a missão de controlar a Administração pública de fazê-lo, respondendo, por sua vez, ao titular maior do poder em uma democracia: o povo.

Convém assinalar ainda que, de acordo com a terminologia anglo-saxônica, além de *control* e *oversight*, há ainda o controle realizado por revisão (*review*). Neste ensaio, consideraremos “controle” como gênero, enquanto *oversight* é aquela forma de controle realizada ao longo de todo o processo de execução dos atos da Administração (*a priori*, durante a execução, e *a posteriori*) e *review* se dá sempre posteriormente. Em termos de controle externo realizado pelo poder legislativo, *oversight* é mais comum em sistemas presidencialistas ao passo que nos modelos parlamentaristas o instituto da *review* é recorrente.

Em países que vivenciaram, no passado recente, governos autoritários, a necessidade de adequar os serviços de segurança estatais ao regime democrático

## Gestão de Inteligência em las Américas

passa pelo desenvolvimento de mecanismos eficientes e eficazes de controle das atividades por eles exercidas. O controle contribui não só para que se evitem abusos por parte desses órgãos, mas também, e isso é muito importante, para modificar sua cultura organizacional e a percepção que a sociedade civil em geral tem dessas instituições, de seus agentes e da atividade que exercem.

O controle da atividade de inteligência compreende mecanismos legais que estabeleçam as diretrizes e os limites para a atuação dos serviços secretos e, também, instituições competentes para o exercício desse controle. Como arcabouço legal, pode-se assinalar desde normas constitucionais que disponham sobre direitos e garantias individuais e limites gerais à atuação do Poder Público, até leis e ordens executivas, passando, ainda, por regimentos internos das organizações, códigos de ética e instruções e diretrizes emanadas por órgãos superiores e pela chefia da agência de inteligência.

No que concerne a pessoas, instituições e níveis de controle, tem-se na própria agência ou unidade de inteligência a primeira instância do controle, de caráter interno e gerencial. Nesse contexto, a chefia, em diferentes escalões hierárquicos,<sup>149</sup> tem um papel fundamental para garantir que o pessoal de inteligência atue de conformidade com os preceitos constitucionais e legais e as diretrizes para o órgão. Ainda em âmbito interno ao Poder Executivo, há o controle exercido por pessoas e instituições não pertencentes à agência, como inspetores gerais, controladorias e, naturalmente, o ministro ao qual se subordina o serviço secreto.

Além do controle interno ao Executivo há aquele externo, exercido por outro Poder (como o Judiciário ou o Legislativo) ou por instituição independente (no Brasil, o Ministério Público). Esse controle externo é essencial para a garantia do equilíbrio entre os poderes, especialmente em sistemas presidencialistas, de “freios e contrapesos”. Por último, há o chamado “controle popular”, exercido pela sociedade civil por meio de suas instituições (como a imprensa, associações e grupos organizados) ou diretamente pelo cidadão (por exemplo, quando denuncia irregularidade cometida pelo serviço secreto ou recorre ao Judiciário em defesa de direito próprio ou alheio que entenda violado).

Em síntese, o controle da atividade de inteligência pode-se dar, basicamente em quatro níveis:



- nível 1: agencial (internamente ao próprio serviço secreto);
- nível 2: interno (feito no âmbito do Poder Executivo, por outros órgãos da Administração pública e pelo Ministro de Estado ao qual a agência de inteligência está subordinada);
- nível 3: externo (realizado pelo Poder Judiciário, pelo Poder Legislativo e/ou por um ente independente, como o Ministério Público no Brasil);
- nível 4: popular (a cargo do cidadão individualmente ou de organizações da sociedade civil).

### Dificuldades de controle da atividade de inteligência

Glenn Hastedt identifica como primeira dificuldade para a fiscalização e o controle da inteligência a questão do sigilo inerente à própria atividade.<sup>150</sup> De fato, aspecto central da questão repousa no segredo, requisito essencial para a eficiência do trabalho desenvolvido pela inteligência. Os serviços de informações não podem simplesmente revelar suas atividades, produtos (e algumas vezes até sua organização) publicamente sem que isso lhes gere grande vulnerabilidade, inclusive diante de seus congêneres, adversos e, principalmente, de seus alvos.<sup>151</sup>

Um segundo problema identificado por Hastedt diz respeito ao fato da atividade de inteligência ainda ser muito mais uma arte (*craft*) que uma ciência. Devido a isso, os profissionais de inteligência tendem a avocar para si certa discricionariedade no exercício de suas funções, decisões sobre linhas de análise ou condução de operações, elaboração de planos ou mesmo interpretação de dados. Daí que os profissionais de inteligência teriam pouca confiança no conhecimento e na competência de seus controladores, sobretudo se esses não tiverem vínculos anteriores com a atividade nem forem assessorados por quem os teve.

Fundamental, portanto, que haja nos órgãos de controle pessoal capacitado com conhecimento (e, se possível, experiência prática) sobre a área de inteligência. Isso é importante mesmo para que seja possível a identificação de condutas irregulares por parte dos controlados. Em outras palavras, aquelas a quem contas são prestadas devem saber sobre o que inquirir.

## Gestión de Inteligencia en las Américas

Terceiro aspecto apresentado por Hastedt diz respeito ao desinteresse dos políticos em se envolverem com a atividade de inteligência. É consenso entre os autores que estudam o tema que “inteligência não dá voto”, mas pode comprometer uma eleição<sup>152</sup> e, por isso, políticos preferem não se envolver com o assunto.<sup>153</sup> Daí a relutância de certos legisladores e até autoridades do Executivo de lidarem com os serviços de inteligência, o que pode provocar uma ausência de controle ou sua fragilização.

Hastedt assinala outro problema relacionado ao controle da atividade de inteligência. Segundo ele, o debate acerca de como controlar a inteligência complica-se pelo fato dos envolvidos terem diferentes opiniões sobre “o problema da inteligência”. Assim, enquanto alguns percebem o controle como essencial para prevenir que os serviços de inteligência se engajem em atividades ilegais, outros aceitam que leis sejam até desconsideradas pelos oficiais de inteligência em prol de valores maiores, como a segurança nacional.<sup>154</sup>

De toda maneira, o que é importante estar claro é que deve haver controle, mas também esse controle não pode constituir obstáculo para a atividade de inteligência, imprescindível para o Estado.<sup>155</sup> Afinal, a atividade envolve a salvaguarda da segurança nacional e, em última análise, a sobrevivência do Estado.<sup>156</sup> Além disso, ainda que o controle tenha deficiências, não se pode falar em democracia consolidada se os serviços de inteligência não estiverem sujeitos à fiscalização e controle dos governantes eleitos.<sup>157</sup>

No que concerne ao controle externo, em especial o realizado pelo poder legislativo, tem-se ainda a legitimação da atividade de inteligência, uma vez que os controladores podem ser bons avalistas dos órgãos de informações. Entretanto, nesse último caso, pode-se estar diante de um dos “paradoxos do controle da atividade de inteligência”.

### Paradoxos do controle

Em um estudo sobre os aspectos gerais do controle da atividade de inteligência, convém fazer referência aos “paradoxos” assinalados por Marina Caparini.<sup>158</sup> São quatro, ilustram bem a relação entre a inteligência e aqueles com função de controlá-la, e podem ser percebidos em diferentes sistemas.

O primeiro paradoxo refere-se à dependência do controlador de informação fornecida pelo controlado, pois, para realizarem um controle efetivo, os

controladores têm que saber o que inquirir. Diferentemente de outras áreas, há pouca possibilidade de se desenvolver conhecimento sobre a atividade de inteligência a partir de fontes externas. Assim, aqueles que controlam, particularmente os políticos, acabam muito dependentes das informações fornecidas pelos próprios serviços de inteligência que fiscalizam.<sup>159</sup> Mesmo nos EUA, esses problemas dificultam o efetivo controle da inteligência por parte do Congresso. É o que assinala Amy Zegart, em recente trabalho sobre as dificuldades do controle externo dos serviços secretos naquele país.<sup>160</sup>

De fato, Zegart assinala que as dificuldades dos legisladores em controlar a comunidade de inteligência relacionam-se a duas deficiências institucionais básicas: a expertise limitada e a fragilidade do poder sobre o orçamento dos serviços secretos. Nesse sentido, Zegart destaca que é difícil se realizar um efetivo controle quando as atividades estão sob um manto invisível e de complicado acesso mesmo para os legisladores. E lembra a assertiva de Max Weber, segundo o qual “os agentes públicos de carreira (não-eleitos) conhecem mais sobre suas organizações que os políticos que as fiscalizam”. Zegart segue então observando deficiências como a falta (ou baixa quantidade) de pessoas oriundas da comunidade de inteligência tanto entre os parlamentares quanto entre as equipes que os assessoram e a pouca familiaridade com um tema que é por si mesmo hermético. Não haveria, tampouco, grupos externos e independentes da comunidade de inteligência que pudessem fornecer subsídios aos legisladores para o exercício do controle. A dependência das informações fornecidas pelos controlados é, praticamente, absoluta.

Como segundo paradoxo tem-se a idéia de que o controlador pode se tornar um significativo aliado<sup>161</sup> ou adversário ferrenho do controlado, o que pode ter grande impacto não só na fiscalização como no fluxo de informação no processo. Um relacionamento antagônico entre controlador e controlado, sobretudo no controle externo, certamente cria barreiras na comunicação e dificulta o controle. Claro que a outra face da moeda é que os controladores sejam demasiadamente condescendentes com os controlados a ponto de não os fiscalizarem realmente. Esse paradoxo pode encontrar soluções no amadurecimento das instituições democráticas, particularmente no que concerne à consciência dos homens públicos das suas funções e da importância de valores democráticos em suas atividades. Entretanto também é paradoxal que, para que isso ocorra, deva ser desenvolvida uma cultura ética que influencie

## Gestão de Inteligência em las Américas

na mudança de algumas práticas institucionais, o que não é nada simples. A situação é agravada porque o tema inteligência não só desperta pouco interesse por parte dos legisladores como também pode lhes causar constrangimentos e antipatias junto a seus eleitores ou mesmo desviar sua atenção de outros assuntos mais palpáveis e relacionados a situações que afetem mais diretamente a vida daqueles que os elegeram.

Outra questão paradoxal tem a ver com a dicotomia controle funcional *versus* controle institucional. Usualmente, fiscalização e controle são feitos com base em um mandato institucional, ou seja, os órgãos de controle fiscalizam determinadas instituições e não a atividade em si. Entretanto, cada vez mais as funções de segurança nacional, inclusive de inteligência, distribuem-se entre diversas agências, órgãos, setores e departamentos da Administração pública, de modo que um controle institucional (voltado para uma agência ou órgão específico) acaba deixando de lado outras tantas organizações que se ocupem do tema. Para a resolução do problema, Reg Whitaker sugere a migração do controle do institucionalismo para o funcionalismo. Assim, a fiscalização se daria em virtude da atividade exercida, independentemente do órgão que a realizasse.<sup>162</sup>

O último paradoxo assinalado por Caparini refere-se ao do sigilo *versus* interesse público. Nesse sentido, convém destacar que: 1) o sigilo é fundamental para o êxito da atividade de inteligência, e o êxito é um interesse público; 2) entretanto, restrições ao acesso à informação inibem o debate público e as iniciativas de controle social; 3) os serviços tendem a “sobreclassificar de maneira indiscriminada” ou “supervalorizar” o conhecimento produzido, as fontes e mesmo os dados brutos, bem como resistem à desclassificação de documentos, o que dificulta a transparência e pode conduzir à “erosão da disciplina”.<sup>163</sup> Diante desse quadro de excessiva restrição à divulgação de inteligência, a reação mais comum costuma ser um aumento no “vazamento” de informações. As razões para isso vão de real preocupação com a ilegalidade e a violação de princípios democráticos a interesses pessoais (motivados, por exemplo, por necessidade financeira, descontentamento com a instituição ou rivalidades internas). O destinatário costuma ser a imprensa, vista como guardiã da transparência.

Comentando esse assunto, Zegart<sup>164</sup> observa a dificuldade mesmo dos próprios parlamentares em acessarem documentos e informações produzidos

ou de posse da comunidade de inteligência. E cita mesmo o órgão mais importante do Congresso dos EUA no que concerne ao controle de contas, o *Government Accountability Office* (GAO), equivalente aos Tribunais de Contas de certos países latino-americanos, tem sido proibido de realizar auditorias na CIA e em outras agências de inteligência sob o argumento do imperativo de segurança nacional. E relata que isso acontece ainda que haja mais de mil funcionários do GAO com credencial de segurança para acessar documentos ultrassecretos e pouco mais de setenta autorizados a conhecer as informações de mais alto grau de sigilo, as *sensitive compartmented information* (SCI). Os parlamentares, por sua vez, têm acesso limitado a esses documentos, sendo-lhe vedado a seus assessores pessoais (ainda que disponham de credencial de segurança) qualquer contato com muito do que é produzido pela comunidade de inteligência. Assim, conclui Zegart, o controle externo fica muito limitado.

### Princípios do controle aplicados à atividade de inteligência

Cada país tem seus distintos sistemas de inteligência e respectivos mecanismos de fiscalização e controle, ditados pela cultura e tradições políticas específicas de cada nação e da sociedade que a compõe. Nesse sentido, Peter Gill destaca que não adianta sugerir que os Estados escolham entre modelos de controle que já funcionem em determinado lugar, uma vez que instituições políticas não podem ser simplesmente transplantadas de um sistema para outro.<sup>165</sup>

Mais importante que a reprodução de um modelo institucional é a adoção de certos procedimentos e princípios gerais que podem ser aplicados em distintos países e regimes. De acordo com Ugarte,<sup>166</sup> aspectos fundamentais do controle da atividade de inteligência encontram-se na resposta às seguintes perguntas: o quê controlar? Por quê, e para quê e com quê finalidade é necessário controlar essa atividade? Como e com quê meios esse controle será exercido e com quê objetivos? A partir desses aspectos, podem ser desenvolvidos mecanismos eficientes de fiscalização e controle.

No que concerne aos princípios de controle, Gill relacionou alguns aplicáveis à atividade de inteligência. Apesar de gerais, não são, entretanto, absolutos nem excludentes, e se aplicam a três dos quatro “níveis de controle” aqui citados: o agencial, o interno ao Executivo e o externo.

O primeiro princípio geral dispõe que tanto o controle gerencial (*control*) quanto o controle externo (*oversight*) são aplicáveis a todos os níveis de

## Gestión de Inteligencia en las Américas

fiscalização, exceto ao controle popular. Assim, se o controle externo é cabível no nível agencial, o controle gerencial também se encontra presente nas atribuições do órgão externo (por exemplo, quando o Congresso autoriza previamente uma operação de inteligência ou aprova recursos para tal).

Como segundo princípio geral está a idéia de que quem produz a inteligência não pode ser o mesmo ente que a fiscaliza. Isso não quer dizer que aqueles que são responsáveis pelas operações de inteligência não devam considerar a legalidade e o respeito aos direitos e garantias individuais em suas condutas. Entretanto, assinala Gill, “é ingênuo acreditar que ministros ou funcionários desejem sujeitar suas ações ao efetivo controle”.<sup>167</sup> Daí a importância tanto de mecanismos legais quanto de princípios éticos arraigados nas instituições de inteligência para coibir eventuais desvios de conduta por parte do pessoal da área e, ainda, ordens manifestamente ilegais.

Associado ao segundo princípio está o terceiro, que preconiza que a obrigação dos responsáveis pelos serviços secretos de estabelecerem claramente padrões e normas que sejam tão públicos quanto possível sem comprometer a segurança. Essas normas e padrões (códigos de conduta, diretrizes, orientações) serão mais detalhados à medida que o nível de controle se aproximar mais do âmbito interno à própria agência. Registre-se que a questão da necessidade de um arcabouço normativo abrangente torna-se ainda mais importante em países que adotam o sistema jurídico de origem romano-germânica, como é o caso do Brasil e de outras nações latino-americanas.<sup>168</sup> Sem leis (no sentido amplo) claras para orientar e limitar atuação dos serviços de inteligência e segurança, o risco de abusos é muito alto. E, repita-se, essas normas têm que ser públicas, conhecidas de todos.

Um quarto princípio baseia-se no controle político. Assim, cada sujeito passivo responde ao sujeito ativo do nível superior, a partir do interno à agência. Por exemplo, a agência ou serviço de inteligência (nível 1) é o sujeito passivo do controle que tem como sujeito ativo um órgão do Poder Executivo externo a ela (nível 2). Isso é mais claro de ser percebido em regimes parlamentaristas, onde há uma seqüência clara de transferência de autoridade do Parlamento para o Poder Executivo (Gabinete) e deste para a Administração (burocracia). Não se aplica com tanta precisão em modelos presidencialistas. Ademais, o órgão do nível 1 está sujeito ao controle simultâneo tanto das entidades do nível 2 quanto dos níveis 3 e 4.

Há um quinto princípio segundo o qual cada entidade controladora reporta-se à autoridade executiva do seu nível. Ou seja, explica Gill, um ente fiscalizador externo à agência, mas interno ao Poder Executivo, reporta-se ao ministro responsável pelo controle daquele nível. Sobre esse aspecto, em países como o Brasil há a dificuldade generalizada de se perceber essa relação no que concerne às competências de controle de uns poderes sobre os outros (por exemplo, da necessidade do Executivo se reportar e prestar contas ao Legislativo) e da Administração (e do próprio Governo) ao destinatário final das atividades estatais, ou seja, à sociedade. Não é à toa que na língua portuguesa não existe equivalência aos termos *accountability* e *enforcement*.

Um último princípio assinalado por Gill é o da necessidade de ampla cooperação entre os órgãos de controle dos diferentes níveis. Essa necessidade se evidencia, sobretudo, quando existe uma comunidade de inteligência (que opere em redes<sup>169</sup>) sob controle mais institucional que funcional. Ademais, ao cooperarem e trocarem informação, os organismos controladores se fortalecem e ao controle como um todo. Certamente essa cooperação entre órgãos de controle não é simples nem fácil. Entretanto, lembra Gill, sem a cooperação, a fiscalização se fragmentará e se tornará menos eficaz. Nesse sentido, caso se queira que o controle das redes de inteligência seja eficaz, então deverá existir também uma fiscalização em rede, ou seja, uma fiscalização funcional.<sup>170</sup>

Derradeira observação de Gill é que tanto as organizações que exercem *control* quanto as que fazem *oversight* devem ter acesso, ao menos potencialmente, à totalidade das informações produzidas pelos serviços fiscalizados/controlados, inclusive as operacionais. Apenas dessa maneira é que os sujeitos ativos do controle terão condições para avaliar corretamente os controlados. Eis a essência da *accountability*.

### Orientações e práticas de controle da atividade de inteligência

Passa-se agora a algumas orientações e práticas para o desenvolvimento de mecanismos de controle da atividade de inteligência. São, em resumo, procedimentos gerais de controle e podem ser consideradas por quem deseje estabelecer um marco legal para a atividade, baseando-se na experiência de vários sistemas pelo mundo, dos modelos canadense e norte-americano aos estabelecidos na Europa Ocidental e nas democracias recentes do Leste Euro-peu, bem como em países da América Latina onde ganha força o controle.<sup>171</sup>

### *Separação do aparato de inteligência em diversas organizações*

Em termos gerais, mecanismo prático importante para o controle da atividade de inteligência, segundo Bruneau e Dombroski,<sup>172</sup> é a separação do aparato de inteligência em diferentes agências, de modo a prevenir que uma única entidade tenha o monopólio da reunião, produção e fornecimento da inteligência. A sugestão é que se distribua a atividade entre órgãos civis e militares, policiais, fiscais ou, ainda, entre agências distintas para inteligência doméstica e inteligência externa.<sup>173</sup>

### *Estabelecimento de mandatos legais para cada organização*

No que concerne à agência ou serviço de inteligência, sugere-se, entre outras coisas, que o mandato da organização esteja claramente definido e limitado a assuntos que sejam detalhadamente explicitados, todos relacionados a ameaças graves à segurança nacional e à sociedade.<sup>174</sup> A competência territorial desses órgãos também deve ser definida com clareza e todo o poder de ação fora do território/jurisdição deve estar acompanhado das correspondentes salvaguardas.<sup>175</sup> Sobretudo em países que vivenciam regimes pós-autoritários, é importante, ainda, que sejam implementadas garantias legais e institucionais com o objetivo de impedir o uso inapropriado do aparato de segurança e inteligência, evitando-se, por exemplo, a partidização do aparato de inteligência ou seu uso contra opositores políticos.

### *Criação de mecanismos de controle relacionados aos dirigentes das organizações*

A figura do dirigente máximo do serviço secreto é de extrema importância para a garantia de que a organização opere em conformidade com os princípios democráticos e seguindo as orientações gerais e específicas para a atividade. Nesse sentido, convém que a legislação estabeleça o processo de designação do diretor (ou diretores) do serviço de inteligência, bem como atributos exigidos a qualquer candidato a ocupar esse(s) cargo(s) e, ainda, fatores que levem à desqualificação do indicado para o posto e à perda do cargo. Se possível, mais de um membro do Gabinete (ou do Governo) deve participar da escolha e designação do diretor (por exemplo, o Presidente ou Primeiro-Ministro e o ministro da pasta ao qual o serviço esteja subordinado). A designação do(s) diretor(es) deve ser examinada e confirmada por um ente



externo ao poder executivo, preferencialmente o poder legislativo ou preposto seu, sendo desejável que a oposição parlamentar participe da indicação ou, no mínimo, do processo de aprovação do nome do diretor. Tudo isso (especialmente os critérios para designação, nomeação e destituição do diretor) deve estar claramente especificado em lei, na qual haja garantias para se evitar que pressões indevidas sejam exercidas sobre o diretor, e também para evitar que ele use seu cargo de maneira inapropriada ou abusiva.<sup>176</sup>

*Regulamentação dos processos de coleta e busca, manuseio de dados e conhecimento e eventual liberação dessas informações ao público*

Outro aspecto fundamental para o controle do aparato de segurança e inteligência do Estado diz respeito à obtenção de dados, produção e manuseio de informações, bem como ao uso e conservação de arquivos pelos serviços de inteligência. A respeito do uso da informação e dos arquivos, é importante que a legislação limite sua reunião e manuseio, bem como o acesso a dados e conhecimentos sobre a vida privada e a intimidade das pessoas. Ademais, é conveniente que haja regras claras referentes a prazos para retenção da informação, uso dos arquivos, acesso a estes, seu manuseio e destruição e, também, garantias de cumprimento dos princípios internacionais de proteção de dados, com auditorias periódicas para fiscalizar o cumprimento da lei. Sobre o assunto, a legislação brasileira de acesso a informações passou por significativas mudanças, sendo a mais recente em 2012, com a entrada em vigor da Lei Nº 12527, de 18 de novembro de 2011, a nova Lei de Acesso à Informação (LAI).<sup>177</sup> Registre-se, preliminarmente, que muitas das alterações da referida lei vão de encontro às boas práticas assinaladas neste ensaio, gerando para a comunidade de inteligência e indo mesmo de encontro a interesses nacionais brasileiros.

Produzida sob a égide do III Plano Nacional de Direitos Humanos (III PNDH), a LAI foi iniciativa paralela à proposição da chamada Comissão da Verdade, proposta no Governo Lula da Silva e estabelecida pelo Governo Dilma Rousseff para apurar violações aos direitos humanos cometidas entre 1946 e 1988 [aí incluído o período militar (1964-1985)]. A LAI, entretanto, parece marcada por um alto grau de revanchismo. O resultado foi uma legislação que dá pouca proteção aos segredos de Estado, que determina a disponibilização na rede mundial de computadores (internet) de todas as informações e documentos sob a guarda do Estado brasileiro, põe

fim à classificação “confidencial” (o que, com a entrada em vigor da Lei, torna automaticamente ostensivos, por consequência, todos os dados, informações confidenciais existentes no Brasil, sem qualquer outro critério para a desclassificação) e estabelece prazos fixos e improrrogáveis para os documentos classificados como reservados (5 anos) e secretos (15 anos). No que concerne aos documentos mais sensíveis, classificados como ultrasecretos, a LAI é taxativa: só podem permanecer classificados por até 25 anos, sendo permitida apenas mais uma prorrogação por igual período.

Assim, com a nova LAI, qualquer documento do Estado brasileiro ou por ele custodiado só pode permanecer sigiloso por, no máximo 50 anos. Isso significa que todos os dados, informações e documentos públicos no Brasil produzidos até 16 de maio de 1962 são, a partir de 16 de maio de 2012, ostensivos e sujeitos a consulta de qualquer interessado, sem que este precise justificar as razões para querer ter acesso a essas informações. Apesar da quase unanimidade junto a sociedade brasileira sobre o caráter positivo da LAI (sociedade que, de fato, pouco conhece os meandros da própria legislação), há aqueles que lhe são críticos, por verem nela um iniciativa irresponsável de permitir acesso irrestrito a toda e qualquer informação, inclusive àquela que pode comprometer os interesses do Estado ou pô-lo em risco e à sociedade.<sup>178</sup>

A atividade de inteligência não deve ser excluída das normas que protegem e asseguram o direito à informação, ressalvado o sigilo relacionado a aspectos de segurança nacional. Nesse sentido, o Poder Judiciário deve ser capaz de examinar a conduta dos órgãos de inteligência também no que concerne ao recurso a poderes especiais. No caso da LAI brasileira, seu art. 21 estabelece expressamente que “não poderá ser negado acesso à informação necessária à tutela judicial ou administrativa de direitos fundamentais” e que “as informações ou documentos que versem sobre condutas que impliquem violação dos direitos humanos praticada por agentes públicos ou a mando de autoridades públicas não poderão ser objeto de restrição de acesso.”

Claro que a implementação de leis de acesso à informação não é algo simples. Note-se, por exemplo, o caso mexicano, em que a *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental* (publicada em 11 de junho de 2002)<sup>179</sup> enfrentou uma série de dificuldades para ser implementada, como o fato de só regular o direito à informação pública governamental em âmbito

federal, deixando para os 31 Estados e o Distrito Federal a tarefa de produzir algo semelhante nos níveis estadual e municipal.<sup>180</sup>

*Estabelecimento de procedimentos especiais para o uso de inteligência oriunda de intercâmbio com organizações estrangeiras*

Questão importante refere-se à inteligência trocada com serviços estrangeiros, ou mesmo com organizações internacionais. Nesses casos, o receptor deve comprometer-se a reter a informação e utilizá-la observando as mesmas regras estabelecidas pela legislação nacional e às condicionantes estabelecidas pela autoridade que a forneceu. No caso brasileiro, a LAI, apesar de seu art. 36 estabelecer que “o tratamento de informação sigilosa resultante de tratados, acordos ou atos internacionais atenderá às normas e recomendações constantes desses instrumentos”, nada dispõe sobre os documentos classificados produzidos a partir desse tratado, por exemplo, no contexto de cooperação entre serviços de inteligência. Isso levou a Comissão de Relações Exteriores e Defesa Nacional (CRE) do Senado brasileiro a suspender, de forma inédita, a tramitação de todo tratado que versasse sobre segurança da informação e intercâmbio de informações sensíveis<sup>181</sup> e recomendar ao Poder Executivo a renegociação de todos os tratados sobre o assunto.<sup>182</sup>

*Estabelecimento de regras sobre direitos de acesso à inteligência*

Na esfera do controle exercido pelo Executivo, é recomendável que a legislação de inteligência contenha regras sobre direitos de acesso diferenciados, quais sejam, o direito do Executivo de acesso à informação em poder do serviço de inteligência, e o direito da chefia do órgão de ter acesso ao ministro que o controla. O ministro, por sua vez, deve ser responsável por formular, total ou parcialmente, as políticas de segurança e inteligência. No caso do Brasil, cita-se o exemplo da Agência Brasileira de Inteligência (ABIN), a qual vincula-se por lei ao Gabinete de Segurança Institucional da Presidência da República (GSI). A Lei Nº 9883, de 7 de dezembro de 1999, estabelece, em seu art. 9º, que “quaisquer informações ou documentos sobre as atividades e assuntos de inteligência produzidos, em curso ou sob a custódia da ABIN somente poderão ser fornecidos, às autoridades que tenham competência legal para solicitá-los pelo Chefe do Gabinete de Segurança Institucional da Presidência da República”.<sup>183</sup>

### *Notificação ao Poder Legislativo sobre operações de inteligência específicas*

Já no que concerne ao controle sobre operações, particularmente as mais intrusivas, é fundamental que estas sejam aprovadas por autoridade competente do Executivo de acordo com a legislação estabelecida pelo Parlamento. Destaca-se a prática de se estabelecer a necessidade de notificação ao Legislativo das operações a serem desencadeadas, o que é importante, sobretudo, em regimes presidencialistas. Bom exemplo disso é a necessidade de consulta à chamada “ganguê dos oito”, grupo de deputados e senadores no Congresso dos EUA que têm credencial de acesso às atividades operacionais mais intrusivas realizadas pela inteligência daquele país.<sup>184</sup>

Assim, no modelo estadunidense, o Presidente da República tem a obrigação de manter as comissões de controle da inteligência do Congresso total e permanentemente informadas sobre todas as operações de inteligência mais sensíveis (*covert actions*), inclusive no que se refere à decisão de desencadeá-las e antes de fazê-lo.<sup>185</sup> Caso o Presidente entenda que uma operação específica possa afetar diretamente os interesses vitais dos EUA, pode limitar essa notificação prévia à “ganguê dos oito”, e a quaisquer outros líderes do Congresso à sua escolha.<sup>186</sup> Foi o que ocorreu no caso da operação que culminou no ataque ao local onde se escondia Osama Bin Laden e na morte do terrorista.

### *Estabelecimento de mecanismos independentes de controle externos às organizações de inteligência*

Quando o controle é exercido por autoridades independentes, externas aos órgãos de segurança e inteligência, mas pertencentes ao Poder Executivo (como o *ombudsman* ou o *Inspector General*), recomenda-se que o funcionário encarregado do controle cumpra requisitos legais e constitucionais para ocupar seu cargo, conte com garantia de inamovibilidade enquanto durar seu mandato, tenha poderes legais suficientes para fiscalizar e controlar questões de fundo e avaliar provas relacionadas às práticas e atribuições dos órgãos de inteligência e, ainda, tenha autoridade absoluta para determinar a forma e o alcance de qualquer ordem, relatório ou decisão que resulte do processo de fiscalização. A lei deve fixar claramente o alcance e o escopo desse tipo de controle, evidenciando a quem (ou a que órgão) o controlador independente deve se reportar (por exemplo, ao ministro ao qual se subordina o serviço secreto, ao órgão de controle ou mesmo ao Chefe do Poder Executivo).

Ainda na esfera do Executivo, o último conjunto de sugestões relaciona-se às salvaguardas contra eventuais abusos ministeriais. Propõe-se, então, que tais salvaguardas estejam claramente estabelecidas pela legislação, assim como as garantias contra a politização dos serviços de inteligência. Entre os mecanismos de salvaguarda estão: 1) a determinação legal que todas as ordens, diretivas e requerimentos do ministro sejam feitas por escrito e conhecidas por um órgão externo de revisão; e 2) a previsão legal de que o ministro deva manter o líder da oposição informado sobre suas principais ações e ordens ao serviço. Claro que essas recomendações e algumas outras que se seguem podem parecer demasiadamente utópicas, mas são sugestões que, se implementadas, poderiam promover mudanças importantes na maneira como os serviços secretos são controlados.

### *Desenvolvimento de serviços de inteligência de Estado, sem orientação político-partidária*

Também em termos de salvaguardas, sugere-se que se estabeleçam mecanismos rígidos para evitar que os serviços de inteligência operem em favor de interesses de qualquer partido ou grupo político. Ademais, não devem atuar para levantar informações sobre atos de protesto, defesa ou dissenso que façam parte do processo democrático e se realizem de acordo com a lei. Isso, entretanto, não pode ser empecilho para que os serviços de inteligência acompanhem organizações que, ainda que legalmente estabelecidas, possam representar ou vir a representar ameaça às instituições democráticas, à segurança nacional e à sociedade.

### *Controle externo exercido pelo Poder Judiciário*

Com referência ao controle externo realizado pelo Poder Judiciário, convém assinalar que o juízo ou tribunal competente para receber denúncias e julgar ações seja constituído de pessoas que cumpram os requisitos legais e constitucionais para ocupar o cargo, não se admitindo, portanto, tribunal ou juiz de exceção. Essas pessoas devem contar com garantia de permanência no cargo enquanto durar seu mandato, e terem competência legal para emitir mandados ou quaisquer ordens vinculantes para se chegar a resultados no processo. Ademais, até onde seja possível, o processo judicial deve ocorrer de maneira transparente e, mesmo em situações em que se exija segredo de justiça, é fundamental que se garanta às partes e a seus representantes legais a maior

## Gestão de Inteligência em las Américas

transparência e o direito de acesso ao processo. No Brasil, por exemplo, a legislação penal e processual garante às partes o acesso ao conteúdo do processo para o contraditório e a ampla defesa, o mesmo fazendo a nova LAI.

### *O papel central do poder legislativo no controle da atividade de inteligência*

É no Parlamento que se encontra a instância máxima de controle externo da Administração Pública e, portanto, da atividade de inteligência. Afinal, juntamente com a produção de leis e a aprovação do orçamento, outra atribuição inerente ao poder legislativo é fiscalizar o poder executivo e os agentes públicos em suas atividades. Esse controle pode ocorrer individualmente, como fundamento da atuação parlamentar, ou pode-se dar por comissões e órgãos do poder legislativo e, ainda, por instituições que não sejam constituídas de parlamentares, mas que atuem apoiando o Parlamento em suas funções de fiscalização e controle.

De maneira geral, os mecanismos de controle à disposição do Parlamento são variados. Compreendem, por exemplo, a competência parlamentar para apresentar requerimentos de informações, por meio dos quais o deputado ou senador pode inquirir uma autoridade pública sobre as atividades por ela exercidas (os as de seus subordinados) e cuja negativa de resposta, em muitos casos, pode gerar sanções – no Brasil, por exemplo, incorre em crime de responsabilidade o Ministro de Estado que se negar a responder a um requerimento de informações no prazo de trinta dias. Essa prática é corriqueira no Parlamento brasileiro.

A legislação brasileira, de maneira semelhante à estadunidense,<sup>188</sup> dispõe sobre a competência dos parlamentares individualmente ou das comissões da Câmara dos Deputados, do Senado Federal e do Congresso Nacional para convocar Ministros de Estado e convidar qualquer cidadão a comparecer perante elas para tratar de temas de interesse do Parlamento.<sup>189</sup> Há, também, as Comissões Parlamentares de Inquérito (CPIs), que, de acordo com o art. 58 da Constituição Brasileira de 1988, “terão poderes de investigação próprios das autoridades judiciais, além de outros previstos nos regimentos das respectivas Casas” e “serão criadas pela Câmara dos Deputados e pelo Senado Federal, em conjunto ou separadamente, mediante requerimento de um terço de seus membros, para a apuração de fato determinado e por prazo certo, sendo

suas conclusões, se for o caso, encaminhadas ao Ministério Público, para que promova a responsabilidade civil ou criminal dos infratores”.

É nas comissões, ainda, que são discutidos e aprovados projetos de lei sobre inteligência e seu controle. Outra atribuição de controle que pode existir em uma comissão é a competência para aprovar nomes do diretor-geral e/ou de outros dirigentes dos órgãos de inteligência. Sobre o assunto, a Lei Nº 9883, de 1999, estabelece a competência do Senado Federal para aprovar o nome do Diretor-Geral da ABIN, indicado pelo Presidente da República.

Ainda no exemplo brasileiro, importante registrar os poderes das CPIs para controlar e fiscalizar a Administração pública. Podem, por exemplo, realizar audiências, públicas ou secretas, para as quais sejam convocados ou convidados autoridades públicas, cidadãos comuns ou representantes de segmentos da sociedade civil. No caso específico de CPIs, pode-se mesmo trazer pessoas coercitivamente para depor como réus ou testemunhas, uma vez que as CPIs têm poderes judiciais em alguns regimes, como no Brasil.

Assim, no Brasil, o controle parlamentar da Administração pública em geral e dos serviços de inteligência em particular se dá por meio de três instrumentos distintos: a convocação de Ministros de Estado,<sup>190</sup> o requerimento de informações,<sup>191</sup> e a realização de audiências públicas.<sup>192</sup> Tratam-se os três de mecanismos de controle inerentes ao poder legislativo e, no caso brasileiro, com previsão constitucional. Todos são amplamente utilizados pelos parlamentares, assinalando o caráter de controle individual do requerimento de informações<sup>193</sup> e o aspecto coletivo dos outros dois procedimentos. No controle da atividade de inteligência, desde a discussão sobre o projeto de lei que criou a ABIN até as crises mais recentes relacionadas ao setor, como a do furto de computadores portáteis da Petrobras que poderiam conter informações sensíveis sobre as reservas de petróleo brasileiras, as autoridades do Poder Executivo têm sido chamadas a prestar contas ao Parlamento por meio de audiências públicas ou reservadas, convocações e requerimentos de informações.<sup>194</sup>

O ideal, de fato, é que haja uma comissão parlamentar específica para atuar como órgão de controle externo da comunidade de inteligência. Essa comissão pode ser mista (composta por deputados e senadores em modelos bicamerais), pode estar em uma das Casas do Poder Legislativo, ou pode mesmo haver duas comissões de controle da atividade de inteligência, uma na Câmara Baixa e

## Gestão de Inteligência em las Américas

outra no Senado. Em todos esses casos, convém que o alcance do mandato da comissão seja horizontal, isto é, sobre todo o setor de inteligência (aí incluídos os departamentos e funcionários auxiliares), e também vertical, incluindo as atribuições de fiscalização e controle baseadas em aspectos como: (a) legalidade; (b) eficácia; (c) eficiência; (d) orçamento e contabilidade; (e) cumprimento de normas nacionais e internacionais de proteção aos direitos humanos; (f) aspectos políticos e administrativos dos serviços de inteligência.

Já no que concerne à composição do órgão de controle parlamentar, é conveniente que a legislação estabeleça de forma clara que esse órgão pertença ao Parlamento, só prestando contas ao próprio Parlamento. Com isso, evita-se a criação de entes de controle compostos por parlamentares, mas “subordinados” de alguma maneira ao Executivo.<sup>195</sup>

Ainda sobre o ente de controle parlamentar, sua composição deve ser de representantes de todo o espectro político, preferencialmente de forma proporcional à composição partidária no Parlamento. Em regimes parlamentaristas, os ministros do Governo devem ser excluídos da lista de possíveis integrantes da comissão de controle, do mesmo modo que se deve requerer aos membros do Parlamento que renunciem a suas funções na comissão caso sejam designados ministros.<sup>196</sup> O presidente do órgão, por sua vez, deve ser eleito pelo Parlamento e ou pelos próprios membros da comissão, e não nomeado pelo Governo. A exemplo do que ocorre no modelo italiano, uma medida interessante é se estabelecer que a presidência do órgão de controle fique sempre a cargo de um membro da oposição. Em outros modelos, a presidência fica com um membro da maioria e a vice-presidência com um representante da minoria. Isso é importante para garantir que órgão de controle exerça suas funções de maneira menos partidária.

O controle orçamentário também é instrumento relevante a serviço do Parlamento. Nesse sentido, recomenda-se que o ente de controle parlamentar tenha acesso a todos os documentos pertinentes ao orçamento de inteligência, mantidas as salvaguardas para que não ocorram vazamentos de informação classificada. Também se defende que a supervisão do orçamento dos serviços de segurança e inteligência seja regida pelos mesmos princípios de bom governo que regulam as outras atividades da Administração pública, com exceções reguladas por lei. Daí que, sob essa perspectiva, a competência para fiscalizar e controlar o orçamento deve ser compartilhada entre a comissão de controle



temática e a comissão de orçamento do Parlamento. Ademais, assinala-se que um Legislativo forte é aquele que tem a prerrogativa de autorizar o orçamento, de modo que os serviços de inteligência só possam utilizar os recursos para os fins específicos autorizados e que não lhes seja permitido transferir ou contingenciar recursos sem a devida autorização legislativa.

Todas as recomendações dos parágrafos anteriores certamente encontrarão resistência para serem implementadas, tanto por parte dos órgãos controlados quanto no próprio parlamento. Afinal, ao se atribuir maiores responsabilidades de controle sobre a inteligência a deputados e senadores, estar-se-á levando esses parlamentares a se inserirem em um mundo politicamente delicado e desagradável em termos eleitorais. Ressalte-se que são raros os membros do poder legislativo interessados em inteligência (e por distintas razões).<sup>197</sup> De toda maneira, em sistemas político-jurídicos de influência romano-germânica, essas transformações começam pelo estabelecimento de legislação que atribua mandatos claros aos órgãos de inteligência e a seus controladores, bem como competências fiscalizadoras expressas a esses últimos. E isso requer, sobretudo, vontade política.

Em se tratando de órgãos não-parlamentares de controle (mas vinculados ao parlamento), os *special review bodies*, exemplos interessantes estão na Austrália, no Canadá e em Portugal. No caso australiano, havia o *Security Appeals Tribunal* (SAT), presidido por um juiz e com função de receber denúncias contra servidores públicos e conduzir investigações sobre candidatos a ocupar cargos públicos. O SAT foi extinto em 1996 e suas atribuições transferidas para o *Administrative Appeals Tribunal* (AAT). Em Portugal, há o Conselho de Fiscalização do Sistema de Informações da República Portuguesa (CFSIRP).

### Efetivando o controle da atividade de inteligência: a experiência canadense

O caso canadense merece especial atenção tanto por seu pioneirismo quanto pelas características daquele modelo. Em 1984, foi aprovado o *CSIS Act*, que criou o *Canadian Security Intelligence Service* (CSIS), um serviço civil, voltado à segurança interna, mas com mandato para realizar inteligência externa em defesa dos interesses canadenses. O *CSIS Act* criou também um órgão independente de controle externo para o CSIS, o *Security Intelligence Review Committee* (SIRC), que deveria se reportar ao Parlamento.

## Gestão de Inteligência em las Américas

Interessante observar que o *CSIS Act* ocorria dentro de um movimento sem precedentes na história canadense de questionamento, por parte da sociedade, das responsabilidades de seu Governo, em particular no que dizia respeito ao papel do Estado frente à salvaguarda das liberdades e garantias individuais. Apenas dois anos antes, em 1982, havia sido aprovada a Lei Constitucional do Canadá, que compreendia a Carta Canadense de Direitos e Liberdades, documento máximo do direito canadense de proteção às liberdades civis e aos direitos individuais. De fato, com o *CSIS Act*, desencadeavam-se mudanças importantes na atividade de inteligência canadense e na maneira como os serviços secretos e a atuação do Estado nessa área eram percebidos e aceitos pela sociedade: modificava-se a cultura nacional sobre inteligência e a opinião pública passava a debater a missão da inteligência e as prerrogativas do Estado na garantia da segurança do cidadão.

Registre-se que as atividades relacionadas à segurança nacional não ficaram exclusivamente a cargo do CSIS. Simultaneamente ao *CSIS Act*, o Parlamento aprovou o *Security Offenses Act*, o qual deu à Real Polícia Montada Canadense (RCMP) jurisdição sobre as questões de segurança nacional relacionadas à execução da lei (*law enforcement*). À medida que aumentaram as preocupações com o terrorismo, cresceu também o número de agências e departamentos com atribuições em segurança nacional e em inteligência.

Fundamental e inovador na nova lei foi a explicitação dos mecanismos de *accountability*, fiscalização, controle e revisão. O *CSIS Act* dedica toda a Parte III de seu texto – seções 29 a 56 (de um total de 56 seções) – ao controle do CSIS, tanto no âmbito do Executivo quanto do Legislativo – aí incluído o SIRC, suas prerrogativas e atribuições. Há, também, a Parte II (seções 22 a 28), voltada ao controle exercido pelo Judiciário. Some-se a isso referências às práticas de *accountability* ao longo das outras seções, como, por exemplo, as determinações legais para que o Diretor do CSIS informe tanto o Ministro quanto o SIRC sobre os documentos enviados ao *Attorney General*, e para que o Ministro envie cópia ao SIRC de suas orientações ao Diretor do CSIS.<sup>198</sup> Portanto, a maior parte do texto da lei (cerca de dois terços) volta-se às diferentes modalidades de controle da atividade de inteligência conduzida pelo CSIS.<sup>199</sup>

A grande inovação em termos de controle externo produzida pela legislação canadense foi a criação do *Security Intelligence Review Committee* (SIRC). O SIRC é um órgão externo de revisão das atividades do CSIS, que se reporta

diretamente ao Parlamento. É o único órgão com mandato legal para conduzir a revisão independente e regular das atividades do CSIS.<sup>200</sup> Seu papel tem sido entendido como de uma instância encarregada de assegurar ao Parlamento e à sociedade canadense que o serviço de inteligência está cumprindo plenamente seu mandato tanto no que concerne à segurança do Estado quanto na preservação, em suas atividades, dos direitos e garantias individuais. Para cumprir esse objetivo, o SIRC supervisiona as atividades-fim do CSIS e investiga as reclamações e denúncias contra o serviço.

O mandato do SIRC é definido nas seções 38 e 39 do *CSIS Act*. Compete ao órgão de controle externo conduzir revisões das atividades-fim do CSIS no desempenho de suas funções.<sup>201</sup> Outro aspecto importante do mandato do SIRC consiste em assegurar que as atividades do CSIS sejam conduzidas de acordo com a Lei, com os regulamentos e as instruções do Ministro, e que o Serviço não esteja realizando suas atividades de maneira arbitrária, excessiva ou desnecessária. Nesse sentido, a preocupação envolve claramente a necessidade de garantia da segurança por meio da atividade de inteligência conduzida pelo CSIS diante da consciência de que abusos não podem ser cometidos, mas que determinados grupos usam o escudo da proteção aos direitos e liberdades individuais para ameaçar o Canadá e seus aliados.<sup>202</sup> O SIRC pode, ainda, examinar os relatórios do Inspetor-Geral do CSIS para verificar questões particulares e apresentar suas próprias conclusões e recomendações às atividades do CSIS.<sup>203</sup>

Ao SIRC compete, ademais, investigar duas categorias de reclamações: as relacionadas a “quaisquer atividades do Serviço” e as sobre recusas relativas a credenciamento de segurança de servidores públicos, candidatos a cargos públicos ou particulares que celebrem contrato com o governo.<sup>204</sup> Há no Canadá, ainda, os Comissariados, geralmente com a função de apurar denúncias ou avaliar queixas contra as organizações sob sua jurisdição, como os Comissários canadenses para a *Communications Security Establishment* (CSE) e para RCMP.

São essas algumas sugestões para o estabelecimento de mecanismos eficientes de controle dos serviços de segurança e inteligência. Claro que é pouco provável que todas sejam adotadas em um modelo. Ademais, a elas podem ser acrescentadas outras, oriundas da experiência de outros sistemas políticos e de controle e que levem em consideração a realidade com que se lida. Não

## Gestão de Inteligência em las Américas

obstante, essas orientações podem servir para qualquer nação que resolva criar mecanismos de fiscalização e controle da atividade de inteligência.

### Conclusões

Sociedades que passaram recentemente por períodos autoritários costumam ver a atividade de inteligência com desconfiança, temor e até aversão. Isso se deve, geralmente, aos vínculos entre os serviços secretos e o aparato repressor das ditaduras. Cria-se, dessa maneira, uma percepção deturpada do papel da inteligência na defesa do Estado e da própria sociedade.

Na América Latina, o controle da atividade de inteligência depara-se com problemas estruturais que intensificam os paradoxos citados neste ensaio. Esses problemas relacionam-se ao passado autoritário recente, durante o qual, em diversos países do continente, o aparato de inteligência foi utilizado contra a sociedade em apoio a governos autoritários. Ademais, em sistemas jurídicos de influência romano-germânica e positivista, mudanças só podem ser desencadeadas com a implementação de novos arcabouços legislativos. E, nesses casos, duas situações podem ocorrer.

Primeiramente, a inércia legislativa e a falta de interesse da sociedade suficiente para pressionar os legisladores fazem com que não sejam aprovadas novas leis na área de inteligência. A consequência é que o assunto permanece sem regulamentação ou com lacunas legais que acabam permitindo significativa discricionariedade na atuação dos serviços secretos e baixo controle por parte do Parlamento.

Uma segunda situação que pode ocorrer é a aprovação de leis que, na prática, tenham poucos efeitos. Nesses casos, cria-se uma camada superficial de legalidade no sistema jurídico, mas com pouca efetividade em termos de controle. É o que tem acontecido, por exemplo, no Brasil, onde, apesar da previsão legal de um órgão de controle externo da atividade de inteligência no Parlamento, a legislação não dá suporte suficiente para o exercício efetivo do controle, ao mesmo tempo em que é baixo o interesse político em controlar os serviços secretos gera pouco envolvimento dos legisladores com o tema.

Além do controle interno organizacional (agencial) e daquele feito pelo Poder Executivo, e ainda do controle externo a cargo de autoridades judiciárias, legislativas ou outras independentes, há um quarto nível de controle realizado

pela sociedade civil, ou seja, pelo povo. Esse chamado controle popular pode ocorrer por meio de grupos organizados de cidadãos (reunidos, por exemplo, em associações, sindicatos ou organizações não-governamentais) ou individualmente, e.g., quando alguém apresenta um reclamação ou entra com uma ação contra os serviços secretos. O controle popular também se pode dar por meio de requerimentos fundamentados em leis de acesso à informação (como a LAI brasileira). A existência de algumas ou de todas essas formas de controle popular assinala o nível de maturidade atingido por um país, em termos de instituições democráticas. Quando é possível ao povo controlar diretamente a comunidade de inteligência, tem-se aí um sinal claro aos serviços secretos para que operem em conformidade com princípios democráticos.

Fiscalizar e controlar os serviços secretos não é tarefa fácil em uma democracia. Mesmo em países como os EUA e o Canadá, onde o controle externo dos serviços secretos tem décadas de tradição, há problemas de efetividade nessa função parlamentar. De fato, controlar externamente a inteligência é algo difícil e que exige um esforço dos parlamentares o qual muitas vezes não estão dispostos a deprender.

De toda maneira, o controle dos serviços secretos é importante ferramenta de aperfeiçoamento das instituições democráticas. Sem ele, abusos podem ocorrer por parte da comunidade de inteligência, muitas vezes com consequências danosas para a própria democracia.

O que se buscou neste ensaio foi se apresentar um panorama geral do controle da atividade de inteligência e de seus paradoxos. Também se tentou sugerir alguns mecanismos para aprimorar esse controle. Note-se que nem sempre esses mecanismos poderão ser aplicados em sua plenitude, pois cada país tem suas particularidades político-jurídico-institucionais. O que é importante ter em mente, em todos esses casos, é que ter serviços de inteligência sob controle, especialmente externo, é mais salutar que não tê-los.

### Biografia do autor

**Joanisval Brito Gonçalves** é Consultor Legislativo do Senado Federal do Brasil para a área de Relações Exteriores e Defesa Nacional e Consultor para a Comissão Mista de Controle das Atividades de Inteligência do Congresso Nacional (CCAI), advogado e professor universitário. Foi analista de informações da Agência Brasileira de Inteligência. Doutor em Relações Internacionais pela Universidade de Brasília (UnB) e Especialista em Inteligência de Estado pela atual Escola de Inteligência (ESINT) brasileira, dedica-se há mais de uma década a estudos e pesquisas na área de inteligência, sendo membro de instituições nacionais e internacionais que tratam do tema. É professor em cursos de inteligência pelo Brasil, entre os quais a Escola Superior do Ministério Público de Minas Gerais, a Escola de Inteligência Militar do Exército, a Academia Nacional de Polícia (do Departamento de Polícia Federal), o Instituto Legislativo Brasileiro e a Escola Superior de Advocacia do Distrito Federal. Tem diversas publicações no Brasil e no exterior sobre atividade de inteligência, entre as quais os livros *Atividade de Inteligência e Legislação Correlata e Políticos e Espiões – o controle da atividade de inteligência*, ambos publicados pela Editora Impetus. Os conceitos e opiniões aqui emitidos são exclusivamente do autor e não refletem necessariamente as posições de entidades às quais esteja vinculado. E-mails para contato: joanis@senado.gov.br e joanisval@gmail.com.



## Estado de Supervisión y Control Democrático de los Servicios de Inteligencia

Russell G. Swenson y Carolina Sancho Hirane

El tema “estado de la supervisión y el control democrático” aborda el nivel de desarrollo de la supervisión y el control de las acciones de los servicios de inteligencia tomadas dentro de los respectivos países del hemisferio. La acción de los servicios de inteligencia en el extranjero tiende a ser de naturaleza clandestina.

Tabla 4 Estado de Supervisión y Control Democrático		
País	Medidas legislativas Poder Legislativo	Medidas judiciales Poder Judicial
Países con revisión legislativa y control judicial previo		
Argentina	Ley de Defensa Nacional 23554 (1988) <sup>205</sup> ; Comisión Bicameral de Inteligencia del Congreso	Ley 27126, Agencia Federal de Inteligencia (2015)
Brasil	Comissão Mista de Controle das Atividades de Inteligência (CCAI)	Los jueces pueden autorizar cualquier interceptación telefónica a las autoridades de policía judicial. La rama judicial recibe quejas sobre actividades de los servicios secretos. El fiscal del Estado controla las fuerzas policiales, pero se mantiene un debate sobre si el fiscal tiene autorización para controlar solamente la investigación criminal o si está facultado también para controlar la inteligencia policial.
Estados Unidos	Comisiones de inteligencia en ambas cámaras del Congreso desde 1976	Ley de Inteligencia sobre Seguimiento de Extranjeros (1978), con enmiendas



Tabla 4, (continua)		
Estado de Supervisión y Control Democrático		
País	Medidas legislativas Poder Legislativo	Medidas judiciales Poder Judicial
Países con sólo revisión legislativa sobre servicios de inteligencia		
Colombia	Comisión Legal (bicameral) Parlamentaria	Ninguna
Países con sólo supervisión judicial sobre servicios de inteligencia		
Costa Rica (existe sólo policía—Fue- za Pública; no hay Ejército)	Ninguna	Decreto 23758 (1994), Capítulo 3, Artículo 13, derogado en 2005.
Países con supervisión democrática sobre servicios de inteligencia, pero no sobre la de las fuerzas armadas		
Canadá	Comisión (independiente) de Re- visión de Inteligencia y Seguridad, (1984 hasta la fecha); informe al Parlamento	Ley del Servicio de Inteli- gencia y Seguridad (1984), Parte 2
Chile	Comisión de Inteligencia en Cá- mara de Diputados	Ley 19974 de 2004. Tribu- nales de justicia autorizan procedimientos especiales de obtención de información.
Ecuador	Comisión Especial de Inteligencia del Congreso	Ley de seguridad Pública y del Estado, 2009
Guatemala	Comisión Especial de Inteligencia del Congreso	Decreto 71 (2005), Artículo 4
Honduras	Ninguna	Será conocida por la Corte Suprema de Justicia cual- quier queja o acusación de violación de la privacidad por parte de la Dirección de Investigación e Inteligencia.

## Gestión de Inteligencia en las Américas

Tabla 4, (continua)		
Estado de Supervisión y Control Democrático		
País	Medidas legislativas Poder Legislativo	Medidas judiciales Poder Judicial
Países con revisión legislativa y control judicial previo		
México	Comisión Bicameral de Inteligencia del Congreso	Ley de Seguridad Nacional (2005), Título 3, Capítulo 2
Perú	Comisión Bicameral de Inteligencia del Congreso	Artículo 20.2 de la Ley 28664 (2005)
Países sin supervisión democrática sobre servicios de inteligencia		
El Salvador	Ninguna	Ninguna
Nicaragua	Ninguna	Ninguna
Paraguay	Ninguna	Ninguna
Uruguay (Ley de inteligencia en debate ante el Congreso 2013-2014)	Ninguna	Ninguna

**Fuente:** Datos tomados de fuentes varias por los editores.

Este esquema de carácter comparativo sobre el estado de supervisión y control de los servicios de inteligencia de varios países en las Américas no deben entenderse como una declaración definitiva, sino una interpretación de las actuales tendencias. Es posible que ciertas medidas burocráticas puedan ser tomadas en cualquier país para lograr objetivos político-militares por la vía de la aplicación de capacidades específicas de inteligencia, especialmente cuando existen una variedad de organismos, que bajo condiciones de emergencia o guerra, uno u otro de éstos puede ser empleado para acciones operativas que puedan evadir la supervisión o el control directo. Por ejemplo, aunque la inteligencia militar está por ley sujeta a la supervisión y control en los Estados Unidos, existen operativos, liderados por la función de inteligencia, donde aviones sin tripulantes, tanto como fuerzas terrestres, han mantenido como objetivo en ciertas partes del mundo al terrorismo, y han sido incluso asesinados ciudadanos estadounidenses. Todo esto nos hace considerar si estas acciones, ordenadas por el presidente de los EE.UU. como comandante en jefe, deben ser objeto de revisión o aprobación por los poderes legislativo y

judicial.<sup>206</sup> Cabe destacar que, si hubieran ocurrido operaciones encubiertas de la Agencia Central de Inteligencia, la rama ejecutiva del gobierno tendría que informar de antemano a las comisiones de inteligencia del Congreso.<sup>207</sup> Así, vemos una instancia de poca, o tal vez, ausente supervisión y control de la inteligencia militar de los EE.UU., en comparación con la certeza de ello respecto a los organismos civiles de inteligencia. Como prueba adicional de cómo varían continuamente las medidas de supervisión y control, las enmiendas a la Ley de Inteligencia para Seguimiento de Extranjeros, de 1978, y específicamente la “Ley Patriótica” han flexibilizado las disposiciones de la Ley de 1978, eliminando, por ejemplo, el requisito que las personas no estadounidenses estén en condición de actuar al servicio de un poder extranjero para poder ser objeto de acciones de recolección (espionaje) de los organismos de inteligencia en cualquier lugar de los Estados Unidos.<sup>208</sup>

Será eficaz la supervisión y el control a la inteligencia en la medida que tomen ventaja los controles y balances entre los poderes legislativo, judicial y ejecutivo: Una vigilancia solamente del ejecutivo no es muy útil. La autoridad civil sobre las Fuerzas Armadas en su conjunto, depende fuertemente del carácter de la supervisión y el control. En el caso de las Fuerzas Armadas permanecen independientes unas de otras, y no bajo la sujeción de una vigilancia civil, por lo que el predominio militar en las decisiones sobre inteligencia continúa. La primacía de la inteligencia militar es tan fuerte que solamente donde existe una comunidad de inteligencia o un sistema de inteligencia que incluya organismos civiles así como servicios de inteligencia militar, cuyos miembros por fuerza de la ley, no pueden tomar decisiones propias relacionadas con la orientación de la inteligencia, y donde exista un control legislativo, nace la posibilidad de una supervisión o control eficaz sobre la inteligencia militar. La investigación más exhaustiva y comparativa relacionada con la supervisión y el control a la inteligencia militar, concluye que la primacía militar en inteligencia es desafiada al irrumpir una reforma al tema de supervisión y control, lo cual ocurre solamente cuando las Fuerzas Armadas desempeñan con poca claridad su misión nacional.<sup>209</sup>

## Ética e Inteligencia: Revisión de la Experiencia Europea y Norteamericana y su Aplicación en América Latina

Carlos Maldonado Prieto

### Introducción

El tema de los principios éticos en la actividad de inteligencia es una cuestión de la mayor importancia y actualidad para el futuro de la profesión. Aunque algunos pesimistas sostengan que el binomio ética-inteligencia sería una contradicción en sí misma, muchos estudiosos y miembros de la comunidad de inteligencia en todo el mundo se encuentran haciendo esfuerzos por demostrar lo contrario.

Los ataques terroristas del 11 de septiembre de 2001 en Estados Unidos, incluyendo las guerras emprendidas en Irak y Afganistán, han revelado una faceta operacional donde los principios éticos han sido puestos en cuestión. La negativa experiencia de los excesos cometidos por agentes de inteligencia en la llamada “guerra global contra el terrorismo” -condiciones aberrantes de encarcelamiento de sospechosos sin juicio en Guantánamo o Abu Ghraib, cárceles secretas, tortura de sospechosos “a distancia”, es decir, efectuada por policías políticas en países árabes alegadamente por encargo de la CIA-, han causado no sólo desazón política sino también un severo cuestionamiento moral. Consecuentemente, una fortísima reacción de autoridades, académicos y de los propios funcionarios de inteligencia, se ha traducido en un replanteamiento de la actividad.

Paralelamente, en Europa Oriental y América Latina, regiones que han logrado superar regímenes políticos autoritarios considerados como residuos de la guerra fría en retirada, se desarrolla un proceso de reforma de los servicios de inteligencia, que incluye la promulgación de leyes que regulan la actividad, intentan profesionalizar a sus integrantes, introducir mecanismos de control parlamentario y judicial, rendición de cuentas, entre otros.

Tras una discusión académica sobre la importancia de la ética en inteligencia y la presentación de algunas experiencias de reforma de servicios de inteligencia, el siguiente trabajo tratará la pregunta de si debe haber un código ético o deontológico en inteligencia como ocurre en otras profesiones como médicos,

abogados o ingenieros. Si así fuera, qué debería contener como elementos mínimos.

### Definiciones conceptuales

La ética tiene como objeto estudiar los actos que el ser humano realiza de modo consciente y libre, o sea, aquellos actos sobre los que ejerce de algún modo un control racional. No se limita sólo a ver cómo o por qué se realizan esos actos, sino que busca emitir un juicio sobre éstos, que permite determinar si un acto ha sido éticamente bueno o éticamente malo. La ética estudia qué es lo moral, cómo se justifica racionalmente un sistema moral, y cómo se ha de aplicar posteriormente a los distintos ámbitos de la vida personal y social. En la vida cotidiana constituye una reflexión sobre el hecho moral y busca las razones que justifican la utilización de un sistema moral u otro.<sup>210</sup>

Se podría decir que una ética propuesta es el conjunto de normas sugeridas por una filosofía o una religión, en tanto que moral vendría a designar el grado de acatamiento que los individuos dispensan a las normas imperantes en el grupo social. En un sentido práctico, ambos términos se hacen indistinguibles y por ello se los considera equivalentes. El matiz que las delimita está en la observación o aplicación práctica de la norma que entraña el mandato ético. Por ello, la norma ética siempre será teórica, en tanto que la moral o costumbre será su aplicación práctica. Asimismo, la moral se basa en los valores que la conciencia nos dicta, a su vez, basada en costumbres aprendidas. Por lo tanto, la moral no es absoluta o universal, ya que su vigencia depende de las costumbres de una región, de la misma manera que la ética tampoco tiene una validez absoluta al ser ambas imperativos hipotéticos.

Por otro lado, la deontología es la ciencia de la moralidad, pues hace referencia a la rama de la ética cuyo objeto de estudio son aquellos fundamentos del deber y las normas morales. Se refiere a un conjunto ordenado de deberes y obligaciones morales que tienen los profesionales de una determinada materia. La deontología es conocida también bajo el nombre de “teoría del deber”.

De allí surge la deontología profesional, que referencia al conjunto de principios y reglas éticas que regulan y guían una actividad profesional. Estas normas determinan los deberes mínimamente exigibles a los profesionales en el desempeño de su actividad. Por este motivo, suele ser el propio colectivo

## Gestión de Inteligencia en las Américas

profesional quien determina dichas normas y, a su vez, se encarga de recogerlas por escrito en los códigos deontológicos. También controla y supervisa, de alguna manera, la integración de nuevos miembros y el adecuado ejercicio de las tareas propias de su profesión. Hoy en día, prácticamente todas las profesiones han desarrollado sus propios códigos. Esto ocurre entre médicos, abogados, periodistas, etc. Para mantener el cumplimiento del código deontológico de las distintas profesiones es habitual la creación de un colegio profesional. Las normas dictadas en el código deontológico son previamente pactadas y aprobadas de manera común y unánime por todos los miembros de la profesión para la cual se elaboran. Son, por tanto, pautas de conducta a seguir cuyo objetivo es realizar un determinado trabajo de forma correcta, adecuada y eficiente.

En el caso de las profesiones que se realizan en el ámbito del Estado, y debido a las posibles repercusiones de perspectivas y acciones indebidas, los preceptos éticos deben ser aun más firmes. Esto rige, por ejemplo, para los militares y los funcionarios que se ocupan de hacer cumplir la ley, es decir, policías, jueces, fiscales y otros semejantes y, por extensión, para los integrantes de la comunidad de inteligencia, tomando en cuenta que la inteligencia inicialmente se trató de un oficio ejercido principalmente por militares. Desde el siglo XIX comenzaron los esfuerzos por humanizar la guerra introduciendo determinados preceptos éticos mínimos para preservar la vida de los heridos, de los prisioneros y salvaguardar la integridad física de la población civil no combatiente. Estos conceptos éticos fueron plasmados en las convenciones de Ginebra de 1864, 1906, 1929 y 1949. Asimismo, en 1948 se proclamó la Declaración Universal de Derechos Humanos de Naciones Unidas, que entre otras cosas consagra los derechos civiles y políticos de las personas y prohíbe la tortura y los tratos degradantes.

### La reacción frente al componente de inteligencia en la “Guerra Global contra el Terrorismo”

Luego del ataque a Estados Unidos del 11 de septiembre de 2001 y de la invasión de Irak del 20 de marzo de 2003, se produjo una gigantesca reacción negativa ante las aparentes fallas de los servicios de inteligencia estadounidenses por no prever los actos terroristas y ante la masiva violación de principios éticos elementales de estos mismos servicios amparados en lo que

el Presidente George W. Bush llamó “guerra contra el terror”. Lo interesante a resaltar es que una serie de funcionarios de la comunidad de inteligencia y académicos vinculados con ella comenzaron a hacerse presente con estudios que están dando cuenta en forma crítica y revisionista de estos fenómenos.<sup>211</sup>

No es casualidad entonces que en 2006 se creara en Washington D.C. la Asociación Internacional de Ética de Inteligencia (IIEA). Esta organización ha realizado conferencias anuales en EE.UU. y Gran Bretaña reuniendo a muchos especialistas del mundo anglosajón, de Israel, Francia, India y otros países. Desde 2010 edita incluso la revista *International Journal of Intelligence Ethics*.<sup>212</sup>

Los estudios analizados constatan en primer término que siempre ha habido resistencia en los miembros de la comunidad de inteligencia estadounidense a aceptar que la actividad se guíe por preceptos éticos, lo que probablemente sea extensivo a todos los países que estuvieron envueltos directa o indirectamente en la guerra fría. Se cita el ejemplo de Thomas Braden, un ex agente de la CIA, quien publicó en 1967 el sugerente artículo “I’m Glad the CIA is ‘Immoral’” [Estoy contento que la CIA sea “inmoral”], argumentando que frente al enemigo Unión Soviética cualquier debilidad significaría derrota.<sup>213</sup> O lo dicho recientemente por el juez federal Richard Posner: “La inteligencia es la segunda profesión más antigua, sólo que con menos moral”.<sup>214</sup> Según este pensamiento, que Allison Shelton considera como parte de una corriente filosófica que llama teleológica, de donde arranca el realismo y la teoría de la guerra justa, el objetivo de la inteligencia sería servir a la seguridad nacional y todo se ordenaría bajo ese objetivo. Por el contrario, la corriente deontológica que proviene de la filosofía de Emmanuel Kant, enfatiza lo absoluto de la moral.<sup>215</sup>

Shelton constata que existe una paradoja inquietante, pues mientras “es un hecho que la mayoría (si no todas) las actividades de inteligencia tienen una base legal en Estados Unidos, las mismas actividades violan directamente o ignoran la ley internacional o de otros países. Yo llamo a esta observación paradójica cuando los Estados Unidos se asignan un papel como paladín de la democracia en todo el mundo”.<sup>216</sup>

Por su parte, Pfaff y Tiel consideran que nos enfrentamos a un tema permanente de tensión entre “moderación ética” y “eficacia”. ¿Hasta dónde es éticamente aceptable trasgredir los principios y qué diferencia hay en tiempos de guerra y en tiempos de paz? Un asunto interesante, pues el asesinato en

## Gestión de Inteligencia en las Américas

tiempos de paz es punible e inmoral, mientras que en tiempos de guerra es aceptable. Lo mismo sucede con el engaño (identidad falsa de un agente, por ejemplo) o la mentira. Ésta siempre es moralmente reprochable, pero no siempre incorrecta desde un punto operativo o en términos no morales. Lo mismo sucede con la incitación, el soborno, el chantaje y la apropiación.<sup>217</sup> Estos autores concluyen que

debido a que el trabajo del profesional de la inteligencia es indispensable para las tareas de seguridad nacional del Estado, el espionaje en sí mismo es una obligación moral derivada. Esto significa que debemos renunciar a la idea que de alguna manera el trabajo del profesional de inteligencia no es compatible con los dictados de la moral. Pero dado que el camino al infierno está empedrado de buenas intenciones y las líneas no se cruzan, se hace imperativo el establecimiento de límites morales para que los profesionales de la inteligencia puedan desempeñar sus funciones con la conciencia limpia. Esto no sólo es bueno para el profesional, sino que es bueno para la profesión, y dada la importancia de la profesión, también para la Nación.<sup>218</sup>

Por otro lado, Melvin Goodman, un reconocido ex analista de la CIA con 24 años de experiencia y experto en la Unión Soviética, famoso por escribir en 2008 el libro *Failure of Intelligence: The Decline and Fall of the CIA*, señala que los presidentes de Estados Unidos tienen la culpa de haber politizado a la CIA en las últimas tres décadas. Según Goodman, desde Jimmy Carter nadie se ha atrevido a reformar el servicio. En su opinión los cuatro mayores problemas que han contribuido a la declinación de la comunidad de inteligencia estadounidense son la militarización de la inteligencia que se tradujo en una fáctica dependencia de las prioridades del Pentágono; la falta de control parlamentario; las acciones ilegales del National Clandestine Service de la CIA, creado en 2005, encargado de operaciones especiales militarizadas (de hecho, Goodman aboga por separar claramente el clásico análisis de inteligencia de las operaciones encubiertas, reduciéndolas al mínimo); y el error del servicio de no decirle la verdad al poder político.<sup>219</sup>

Pese a estas opiniones lapidarias, hay que señalar que al menos los Presidentes Franklin Roosevelt y George W. Bush hicieron esfuerzos para sacar lecciones



de las fallas de inteligencia por los ataques a Pearl Harbor en 1941 y a las Torres Gemelas en 2001, y los Presidentes Gerald Ford, Jimmy Carter y Ronald Reagan prohibieron que funcionarios del gobierno –un eufemismo para indicar a los agentes de la CIA- cometieran asesinatos políticos en el extranjero.

Ford se basó en las conclusiones del Comité Church, por el senador Frank Church que lo presidió, que fue establecido por el Senado estadounidense en 1975 y que, entre otros aspectos, investigó la política de intentos de asesinato selectivos de la CIA contra Fidel Castro de Cuba, Patrice Lumumba del Congo, Rafael Trujillo de la República Dominicana, Ngo Dinh Diem de Vietnam del Sur y del general René Schneider de Chile durante las administraciones de los Presidentes Eisenhower, Kennedy y Johnson. El informe Church condenó en duros términos estos abusos: “Consideramos que el asesinato [político] viola los preceptos morales fundamentales de nuestra forma de vida... Rechazamos cualquier noción de que Estados Unidos debe justificar sus acciones por los estándares de los totalitarios”.<sup>220</sup>

De hecho, el Presidente Ford firmó una orden ejecutiva que prohibió los asesinatos. Jimmy Carter hizo lo propio en 1978 y Ronald Reagan lo confirmó con su orden ejecutiva 12333 de 1981. Ésta todavía se mantiene vigente. Sin embargo, en ninguna de las órdenes ejecutivas se explica el término asesinato. Eventualmente podría interpretarse que al menos la primera de ellas fue redactada influenciada por el informe del Comité Church, y que por ello se condenara expresamente el asesinato o el intento de asesinato de líderes políticos extranjeros hostiles a Estados Unidos. Pese a ello no hay absoluta certeza sobre el significado del término en las ordenes ejecutivos porque ninguno de los tres mandatarios hizo comentarios públicos explicando sus actos.<sup>221</sup>

Un segundo tema en debate es la politización de la inteligencia, es decir la anómala relación entre el poder político y los organismos de inteligencia que, en una visión ideal, deberían ser profesionales y asépticos políticamente hablando. Esta discusión se ha centrado en lo que muchos consideran la manipulación política sobre el motivo para iniciar la segunda guerra del Golfo, la supuesta existencia de armas de destrucción masiva por parte del régimen de Saddam Hussein y el papel que le tocó cumplir a la comunidad de inteligencia de Estados Unidos.

Nuevamente Goodman arremete contra la CIA al señalar que sus jefes y analistas más experimentados violaron todas las normas del proceso de análisis

## Gestión de Inteligencia en las Américas

de inteligencia ayudando a la administración Bush a construir la justificación de la guerra contra Irak. “Hay filtros en las direcciones de inteligencia y operaciones para prevenir la introducción de embustes en los productos finales de inteligencia, pero los jefes y los analistas se pasaron una serie de luces rojas”.<sup>222</sup> Esto significó que se utilizó informes desechados sobre compras iraquíes de uranio en Niger para justificar el mensaje del estado de la Nación de 2003. Lo mismo ocurrió con la supuesta conexión entre el régimen iraquí y Al Qaeda y la leyenda sobre la existencia de armas de destrucción masiva en Irak, creyendo las fantasías difundidas por el Comité Nacional Iraquí.

También hay que considerar que la politización de la inteligencia no es un fenómeno exclusivamente estadounidense. El reconocido especialista Erich Schmidt-Eenboom ha revelado las principales transgresiones llevadas a cabo por el Servicio de Inteligencia Exterior de Alemania (BND), para demostrar que incluso las democracias más maduras no están libres de prácticas ilícitas reñidas con la ética profesional. Él considera que

la exigencia de establecer un freno por parte del Estado a la autonomía de los aparatos de inteligencia, se basa en la falsa impresión que se ve aumentada a través de la información sensacionalista de la prensa, de que los servicios de inteligencia actúan a menudo de espaldas al gobierno persiguiendo sus propios fines. Sin embargo, esto ocurre sólo en casos excepcionales.<sup>223</sup>

Asimismo, sostiene que “la supervisión de los jefes de inteligencia y sus subalternos se ejerce conscientemente de manera ligera por parte de la Oficina del Canciller [Primer Ministro]. Con ello se pretende interferir lo menos posible en la eficiencia de los servicios, haciendo la vista gorda cuando éstos sobrepasan los límites legales”.

Este autor detalla exhaustivamente contravenciones, errores, abusos e ilegalidades cometidas por la inteligencia alemana. Entre las más graves se cuentan:

a) **Intervención en el conflicto de la ex Yugoslavia:** El BND trató de proporcionarle armas a las fuerzas croatas en 1994 burlando el embargo de la ONU, y cooperó con el grupo terrorista kosovar UCK;

b) **Espionaje e infiltración de partidos políticos legales:** Desde 2006 aumentan las señales de que el Servicio de Inteligencia Interior (BfV) se dedica a observar con métodos intrusivos a partidos políticos. Es el caso del seguimiento de parlamentarios sajones del NPD (ultraderecha) y del líder del Partido de Izquierda, Oskar Lafontaine. Esto ya había ocurrido en los años noventa cuando el Partido Verde fue observado e incluso infiltrado. El autor sostiene que se trataría de una maniobra de los partidos políticos tradicionales para mantener sin cambios el sistema de partidos;

c) **Observación de periodistas y científicos:** El físico nuclear Klaus Traube fue observado ilegalmente por el BfV en 1975; el BND intervino las llamadas telefónicas del escritor Günther Wallraff en 1976; el BND ha seguido observando a periodistas;

d) **Cooperación con regímenes violadores de los derechos humanos:** En la lucha contra el terrorismo, el BND no ha dudado en cooperar con países –sobre todo árabes– en que se utiliza sistemáticamente la tortura;<sup>224</sup> y

e) **Cooperación con criminales de guerra nazis:** Los archivos de inteligencia han revelado que Klaus Barbie, el “carnicero de Lyon”, cooperó en 1966 desde su refugio en Bolivia con el BND. Este criminal de guerra redactó 35 informes sobre temas políticos –posiblemente sobre venta de armas alemanas a países sudamericanos–, informes que fueron pagados. Además, el BND sabía el paradero de otro criminal nazi, Adolf Eichmann, ocho años antes que los agentes israelíes lo secuestraran en Argentina en 1960.<sup>225</sup>

Una tercera cuestión tiene relación con la profesionalidad, es decir, si los integrantes de la comunidad de inteligencia consideran su quehacer como una profesión o no. Si efectivamente la consideran una profesión, allí surge un segundo tema, pues toda profesión posee generalmente un código de ética que impone determinados límites y comportamientos a la práctica de la misma. Unos autores creen que la inteligencia no necesita un código de ética, otros creen que sí.

Uno que no cree en la necesidad de los códigos es Stefan Brem, que trabaja en la Oficina Federal de Protección Civil en el Ministerio de Defensa suizo, y representa bien el modelo europeo de múltiples controles externos sobre la actividad de inteligencia. Brem considera que es suficiente que haya reglas y

## Gestión de Inteligencia en las Américas

procedimientos claros, un buen control externo, responsabilidad y rendición de cuentas (accountability) y transparencia institucional. Y cita las cinco principales recomendaciones contenidas en el decálogo “Directrices sobre Derechos Humanos y la Lucha contra el Terrorismo” que adoptó el Comité de Ministros del Consejo de Europa en julio de 2002. Acatando estas recomendaciones, ningún servicio de inteligencia podría ser acusado de cometer excesos o contravenciones a una supuesta ética profesional:

a) **Prohibición de arbitrariedades:** Respeto de los derechos humanos, excluyendo toda forma de discriminación o trato racista, y apropiada supervisión de los procedimientos;

b) **Legalidad de las medidas antiterroristas:** Todas las medidas deben ser legales, y cuando una restrinja los derechos humanos, debe ser definida con precisión y ser proporcional al fin perseguido;

c) **Absoluta prohibición de la tortura:** Queda prohibida la tortura y los tratos degradantes en toda circunstancia, en especial durante el arresto;

d) **Provisiones en la recolección y procesamiento de información personal:** Estos procedimientos deben estar cubiertos por la ley interna y ser proporcionales al fin perseguido, y pudieran ser supervisados por una autoridad independiente; y

e) **Medidas que interfieran con la privacidad de las personas:** Medidas como allanamientos, intervenciones telefónicas, uso de agentes encubiertos y otras deben ser objeto de ley y posibles de revisión por un juez, y el uso de la fuerza debe ser proporcional al fin perseguido.<sup>226</sup>

En el caso alemán, Schmidt-Eenboom sostiene que es necesario reforzar los controles políticos para evitar las trasgresiones a la ética profesional. Él ha sugerido la creación de un Inspector de los Servicios de Inteligencia que actuaría como un ente investigador institucionalizado en la Oficina del Canciller Federal. La mera existencia de esta institución tendría un efecto beneficioso en la actuación diaria de los servicios, reduciendo así posibles castigos arbitrarios. Un buen ejemplo ya existe: el Delegado Parlamentario de Defensa que, con plenos poderes, vigila que no se produzcan violaciones de los derechos humanos de los soldados.<sup>227</sup>

En todo caso, la mayoría de los autores consultados, no solamente estadounidenses y alemanes, sino que de muchos otros países, se inclinan por establecer algún tipo de código de ética profesional para las agencias de inteligencia. Un buen ejemplo es el decálogo presentado por Brian Snow, un analista que trabajó por 34 años en la Agencia Nacional de Seguridad (NSA) de Estados Unidos. Según él, este código debería contener al menos once normas de comportamiento:

- a) No dañar a ciudadanos estadounidenses o sus derechos establecidos en la Constitución;
- b) Defender la Constitución y el Estado de Derecho, estando limitados por el espíritu y la letra de las leyes de los Estados Unidos;
- c) La conveniencia no debe ser nunca una excusa para la mala conducta;
- d) Ser responsables de nuestras decisiones y acciones y apoyar los procesos de la rendición de cuentas para asegurar nuestra adhesión a estos principios;
- e) Las declaraciones que hacemos a nuestros clientes, colegas, supervisores y al público estadounidense serán verdaderas, y no concebidas para engañar u ocultar innecesariamente de ninguna manera;
- f) Vamos a tratar de resolver las decisiones éticamente difíciles en favor de los requisitos constitucionales, de la verdad y de nuestros conciudadanos;
- g) Vamos a abordar las posibles consecuencias de nuestras acciones con antelación, especialmente las consecuencias del fracaso, del descubrimiento y las consecuencias no deseadas del éxito;
- h) No vamos a tomar decisiones que imponen un riesgo innecesario a los inocentes;
- i) Si una acción nuestra pudiera dañar a nuestros ciudadanos, solicitaremos la autorización de una autoridad nacional externa a la agencia que esté en su cadena de mando;
- j) Aunque pudiéramos trabajar en secreto, vamos a trabajar de tal modo que cuando nuestros esfuerzos sean conocidos, nuestros conciudadanos no se avergonzarán de nosotros y de nuestros esfuerzos; y
- k) Cumpliremos con todos los acuerdos públicos e internacionales sobre derechos humanos que nuestro país ha ratificado.<sup>228</sup>

## Gestión de Inteligencia en las Américas

Incluso existe el caso de España, donde en 2010 se dio a conocer que el Centro Nacional de Inteligencia (CNI) preparaba un código ético para el desempeño de sus funcionarios.<sup>229</sup> Meses después se supo que además del código de ética se introduciría un control judicial que supone el visto bueno de un juez competente para cualquier cooperación de seguimiento o escucha en terreno interno, un control externo común en la mayoría de los servicios de inteligencia occidentales.<sup>230</sup> Sin embargo, el código, que al parecer está listo hace mucho tiempo (incluye la independencia política –no puede haber militancia activa en partidos políticos- de todos los miembros del CNI y severas sanciones contra la lacra de las frecuentes filtraciones de información), ha sufrido la resistencia de muchos funcionarios que aducen que las nuevas directrices podrían afectar gravemente la operatividad del servicio. El nuevo gobierno conservador de Mariano Rajoy ha asegurado que el código sería aprobado en el más breve plazo.<sup>231</sup>

Por otro lado, también hay los que piensan que los integrantes de la comunidad de inteligencia deben poseer un *ethos* profesional, que sería más amplio y más profundo que un código de ética o deontología profesional, y no puede ser impuesto desde fuera. En esa concepción, según Albert Pierce, académico de la National Defense University de Washington D.C., el *ethos* tiene que ver más con “quién eres” que con “qué haces”, mientras que el código de ética profesional que es una derivación y un desarrollo a partir del *ethos*, y por lo mismo trata de “qué haces”. Es por ello que el *ethos* sería orgánico, en el sentido de que debe crecer desde dentro en un proceso que vaya desde abajo hasta arriba y desde arriba hasta abajo en una organización de inteligencia. En resumen, se debe tratar de un proceso intelectual de introspección al interior del organismo, que dé cuenta de sus funciones profesionales, de su papel en el área de la seguridad nacional y en su especificidad como servicio público y del Estado.<sup>232</sup>

### Una perspectiva ética sobre las reformas en Europa Oriental y América Latina

En los procesos de democratización de los países del llamado socialismo real y de redemocratización de América Latina ocurridos en los últimos veinte años, uno de los puntos más complejos ha sido la reforma de los servicios de inteligencia. Coincidentemente, las cuestiones de ética profesional y de

control político-institucional que han sido objeto de un amplio debate tanto público como especializado en Estados Unidos y en países de Europa Occidental, han tenido gran importancia a la hora de efectuar las reformas y asegurar su éxito. Precisamente de Estados Unidos y de Europa Occidental ha venido buena parte de los impulsos reformadores y los modelos que se han implantado en las nuevas democracias. Se puede afirmar sin ambages que las reformas en inteligencia emprendidas en Europa del Este y en América Latina son tributarias de la discusión sobre ética en inteligencia que se ha descrito en páginas anteriores.

**Una transformación ética: inteligencia como servicio público.** Luego del colapso de la Unión Soviética y la reorientación de sus aliados europeos, se desmontaron los instrumentos represivos del aparato estatal de partido único. En el caso de los servicios de inteligencia, estos países debieron afrontar no sólo el clásico desafío de “democratizar la inteligencia”,<sup>233</sup> es decir, encontrar un adecuado equilibrio entre eficiencia y transparencia, sino que además encarar transformaciones profundas de una práctica antidemocrática desarrollada por décadas. Estos otros desafíos fueron los siguientes: a) un cambio de doctrina, asumiendo que la inteligencia abandonaba la misión de defensa absoluta del Estado socialista, convirtiéndose en un servicio público susceptible de escrutinio público y control externo; b) un cambio normativo, estableciéndose un marco jurídico para el respeto efectivo de las leyes y evitando la injerencia o interferencia de la política; y c) un cambio institucional, organizando adecuadamente la comunidad de inteligencia según las dimensiones del país y sus particularidades, disponiendo de cuadros de mando y personal especializado, y operando con seguridad e independencia política.<sup>234</sup>

En la mayoría de los casos, las antiguas agencias de inteligencia fueron disueltas o reformadas completamente, se promulgaron leyes que reglamentan claramente las funciones de las agencias y se introdujeron controles de parte del ejecutivo, del parlamento y del poder judicial. En Polonia, por ejemplo, las nuevas agencias son supervisadas por un Comité para los Servicios Especiales que radica en el Comité de Ministros. En la República Checa, siguiendo el modelo británico, en 1991 se estableció el Consejo para la Coordinación de los Servicios de Inteligencia. Por su parte, en Hungría, además de los controles ejecutivo, parlamentario y judicial, hay supervisión del Defensor del Pueblo y del Comisionado para la Protección de Datos. En el caso

## Gestión de Inteligencia en las Américas

de Eslovaquia, el nuevo Servicio de Información que existe desde 1993 sólo realiza labores de análisis y no puede detener personas.<sup>235</sup>

**La ética de servicio público fácilmente volteada.** Estas reformas, no siempre fáciles de incorporar en el quehacer cotidiano de las nuevas o remozadas agencias de inteligencia -todavía hoy se evidencian serias falencias como prácticas ilegales, nepotismo, corrupción, clientelismo, chantaje, etc.<sup>236</sup>- fueron acompañadas por el difícil proceso de incorporación de los ex países socialistas a los mecanismos de concertación europea. Esto ha traído consigo a su vez la adopción de cánones de comportamiento democrático que refuerzan el proceso de reformas. De hecho, la mayoría de ellos ya son miembros de la OTAN, de la Unión Europea, de la zona euro y de la Organización para la Seguridad y la Cooperación en Europa (OSCE). Incluso, los más desarrollados económicamente -Eslovaquia, Eslovenia, Estonia, Hungría, Polonia y República Checa- son miembros del exclusivo club de países pertenecientes a la Organización para la Cooperación y el Desarrollo Económico (OCDE).

En el caso latinoamericano, los servicios de inteligencia también adolecen de serias falencias éticas y de instrumentalización política, donde

hay una evidente tensión entre la función de inteligencia y la vida democrática de los países. Los servicios de inteligencia cultivan el secreto, muchas veces no respetan los derechos de los ciudadanos y violan su privacidad. Esto complota contra la legitimidad que debe tener esta función esencial.<sup>237</sup>

Además, la politización o partidización de la inteligencia es un hecho recurrente tanto en la historia como en la actualidad. Esto se expresa en la tendencia al clientelismo político que convierte a las agencias de inteligencia, como muchas otras dependencias del Estado, en botines de ciertas fracciones de los partidos o las coaliciones gobernantes. En casos extremos, los servicios de inteligencia, con todo su acervo instrumental (escuchas clandestinas, espionaje selectivo, informantes pagados, etc.), son transformados en una policía política al servicio de un cierto gobierno y en desmedro de sus opositores.<sup>238</sup>

**La creación de nuevos organismos de inteligencia para estabilizar reformas en comportamiento ético.** El proceso de reformas en inteligencia ha pasado por varias fases, produciéndose avances y retrocesos según la realidad política



de cada país. Una primera ocurrió en el Cono Sur y Brasil luego que acabaron las dictaduras militares. Producto de ello fueron creadas nuevas agencias de inteligencia en Brasil (Agencia Brasileña de Inteligencia, en 1999) y Chile (Dirección Seguridad Pública e Informaciones y Agencia Nacional de Inteligencia, en 1993 y 2004, respectivamente) o completamente reformadas las existentes, como ocurrió en Argentina. Otras fases de reforma han ocurrido posteriormente, en especial al término de gobiernos autoritarios, como en el caso del Perú en 2001; crisis de seguridad, como en Ecuador en 2008; escándalos de corrupción y acciones ilegales, como ocurrió en Colombia a partir de 2005, o por efecto de un cambio de régimen político, como es el caso de México desde el año 2000.

Probablemente, el caso colombiano del Departamento Administrativo de Seguridad (DAS) es el más dramático de todos. Luego de un proceso de prolongado deterioro institucional, que incluyó el enjuiciamiento de directores, jefes y funcionarios, acusados de asesinatos, negocios incompatibles con los paramilitares y la guerrilla, espionaje telefónicos -las famosas “chuzadas”- de jueces, políticos y periodistas, entre otros muchos delitos, y el establecimiento de una Comisión Especial para su reforma en 2005 -que resultó infructuosa-, el DAS, creado en 1953, fue formalmente disuelto y reemplazado por una nueva organización. Se trata de la Dirección Nacional de Inteligencia (DNI), creada a fines de 2011, y que recibirá apoyo especializado de los servicios de inteligencia británicos.<sup>239</sup>

Como señaló lacónicamente el Presidente colombiano Juan Manuel Santos, “es triste pero cierto: los cambios en inteligencia nacen de las crisis. Y hay que saber aprovechar las crisis”. Esta nueva entidad no supondrá solamente un cambio de nombre pues “esta agencia será algo completamente nuevo, que nunca ha existido en el país: una agencia civil dedicada de manera exclusiva a tareas de inteligencia”. La DNI “no tendrá facultades de policía judicial”, tildando de insano que la inteligencia pueda luego llevar a cabo detenciones, una práctica que a su juicio evoca momentos sombríos de las dictaduras del Cono Sur. Agregó que “esta agencia trabajará en silencio por el bien común”, y agregó que “se busca la profesionalización a través de una nueva carrera profesional de inteligencia”.<sup>240</sup>

Paralelamente, el parlamento colombiano aprobó en 2011 una nueva ley de inteligencia y contrainteligencia que garantiza plenamente el respeto de los derechos humanos. Su artículo 4 señala que

## Gestión de Inteligencia en las Américas

la función de inteligencia y contrainteligencia estará limitada en su ejercicio al respeto de los derechos humanos y al cumplimiento estricto de la Constitución, la Ley y el Derecho Internacional Humanitario y el Derecho Internacional de los Derechos Humanos. En especial, la función de inteligencia estará limitada por el principio de reserva legal que garantiza la protección de los derechos a la honra, al buen nombre, a la intimidad personal y familiar, y al debido proceso. Ninguna información de inteligencia y contrainteligencia podrá ser obtenida con fines diferentes de: a) Asegurar la consecución de los fines esenciales del Estado, la vigencia del régimen democrático, la integridad territorial, la soberanía, la seguridad y la defensa de la Nación; b) Proteger las instituciones democráticas de la República, así como los derechos de las personas residentes en Colombia y de los ciudadanos colombianos en todo tiempo y lugar -en particular los derechos a la vida y la integridad personal- frente a amenazas tales como el terrorismo, el crimen organizado, el narcotráfico, el secuestro, el tráfico de armas, municiones, explosivos y otros materiales relacionados, el lavado de activos, y otras amenazas similares.<sup>241</sup>

Asimismo, el artículo 37 se refiere a que la obediencia debida<sup>242</sup> no será aceptada

para los casos en que el servidor público posea información relacionada con la presunta comisión de genocidio, ejecuciones extrajudiciales, tortura, desplazamiento forzado, desaparición forzada, violencia sexual masiva, crímenes de lesa humanidad, o crímenes de guerra por parte de un servidor público. En cualquier caso los servidores públicos de los organismos que desarrollan actividades de inteligencia y contrainteligencia podrán denunciar las actividades delictivas de las que tengan conocimiento de manera directa o mediante representante del organismo de inteligencia y en condiciones que permitan garantizar su seguridad e integridad, garantizando la protección de fuentes, medios y métodos.<sup>243</sup>

Un segundo caso a analizar es el ecuatoriano. Aunque allí no se produjo la masiva represión política que caracterizó al Cono Sur y Brasil, también en Ecuador ocurrieron excesos en la década de los ochenta. Una Comisión de la Verdad investigó las violaciones de los derechos humanos ocurridas en el período 1984-2008 cometidas por elementos de las fuerzas armadas, Policía Nacional y otros organismos del Estado relacionados con el área de la defensa nacional y la seguridad interna, incluidas las agencias de inteligencia. La Comisión comprobó que hubo un total de 456 víctimas, la mayoría de ellas acaecidas entre 1984 y 1988, coincidente con la presidencia de León Febres Cordero y con el período de mayor operatividad del grupo guerrillero Alfaro ¡Vive Carajo!<sup>244</sup>

A raíz del ataque colombiano a un campamento de las FARC en territorio del Ecuador en 2008, se estableció una comisión oficial que investigó los hechos. El informe resultante declaró:

La falta de celeridad con la que actuaron los organismos de Inteligencia del Estado ecuatoriano para dar a conocer al mando político, los graves sucesos acontecidos en territorio nacional, así como la oportunidad y eficacia con la que la Inteligencia colombiana conoció en detalle estos sucesos, hicieron presumir a las más altas autoridades del Gobierno ecuatoriano que existía una campaña de ocultamiento de la información orquestada por organismos de Inteligencia extranjeros.<sup>245</sup>

Como consecuencia de esa crisis se disolvió la Dirección Nacional de Inteligencia en manos de militares y se la reemplazó por la Secretaría Nacional de Inteligencia (SENAIN) en 2009. Sin embargo, su desarrollo institucional ha sido débil y lento, ha sido blanco de críticas -no habría detectado anticipadamente la sublevación policial que remeció al país en septiembre de 2010- y ha tenido una gran rotación de directores, pasando de civiles a militares retirados y viceversa.<sup>246</sup>

**Emergen instituciones internacionales para promover una ethos profesional en inteligencia.** Por último, hay que consignar un caso muy peculiar que se produjo en Chile. En 1993, en plena democracia, la Armada requisó todos los ejemplares de un libro escrito por Humberto Palamara, uno de sus oficiales

## Gestión de Inteligencia en las Américas

en retiro, y lo sometió a juicio, una muestra palpable de las dificultades que debió afrontar la transición democrática en ese país. El autor recurrió de protección a la Corte Interamericana de Derechos Humanos.<sup>247</sup> Ésta sentenció en 2006 que el Estado de Chile había violado los derechos de Palamara por haber aplicado censura previa, violado las garantías del debido proceso al haberlo sometido ilegítimamente a la jurisdicción militar y violado el derecho a la propiedad privada, al impedirle el uso y goce de la obra de su creación intelectual. Además del pago de indemnización y publicación del libro confiscado, el Estado chileno fue comprometido a la adecuación de la jurisdicción penal militar a los estándares internacionales, es decir, que la jurisdicción penal militar debe limitarse a los delitos de función cometidos por militares en servicio activo, de forma tal que en ninguna circunstancia un civil se vea sometido a la jurisdicción de los tribunales penales militares.

En su libro, reeditado finalmente en 2006 -como parte del cumplimiento de la Corte-, Palamara critica severamente la violación por militares de los derechos humanos, la utilización de los servicios de inteligencia militares en la guerra antisubversiva y aborda la necesidad de adecuarlos a ciertos parámetros éticos:

A mi parecer, mientras la inteligencia carezca de un código de conductas éticas, que oriente la actividad de las personas que en ella se desempeñan, se mantendrá vulnerable a satisfacer intereses particulares, de líderes corruptos, que le impedirán alcanzar el prestigio de una profesión. Mientras esta situación no varíe vale considerar a inteligencia simplemente como una actividad o una ocupación, que reúne personas especializadas en los diferentes roles que se deben desarrollar en la actividad de inteligencia.<sup>248</sup>

De acuerdo con este ejemplo, podemos entender que no basta la existencia de una ética admirable de una sola persona de entre los cuadros de inteligencia, sino que su expresión perdurable puede depender del poder más amplio de un conjunto de opiniones expresado por medio de una convención multilateral o internacional. Con este ejemplo, Chile ha innovado en aceptar la decisión de un ente legal multilateral, lo cual puede establecer un precedente en la región respecto al tema de evolución ética en relación a la inteligencia.

## Conclusiones

Una breve descripción de los delitos o excesos que se cometen generalmente en inteligencia, lleva a concluir que hay tres tipos:

a) **Individual:** Los de tipo personal que cometen individuos particulares (robo, espionaje, venta de material sensible, cobro por extorsión, etc.). Éstos pueden ser combatidos con medidas disciplinarias, de seguridad -por ejemplo, mediante oficinas de asuntos internos- y judiciales;

b) **Institucional:** Los que son cometidos por los servicios de inteligencia son producto de fenómenos de exceso de celo, autonomización y corporativismo, generalmente en busca de mayor reconocimiento, lucha de competencias entre agencias o incluso por oposición a la línea seguida por la autoridad. Éstos, por definición, se llevan a cabo sin el consentimiento o el conocimiento de la autoridad política, aunque muchas veces es difícil discernir con exactitud si ésta ha tenido conocimiento o no; y

c) **Político:** Aquellos actos cometidos por mandato de la autoridad política, que se cometen institucionalmente (fabricación de pruebas, persecución de opositores, periodistas, jueces y otros personajes u organizaciones incómodas).

Estos dos últimos delitos, por ser de carácter institucional, necesitan otros métodos para ser combatidos eficientemente. Hay que tener en cuenta que los tres tipos de delitos o infracciones descritas son de común ocurrencia en todo el mundo. Prácticamente no hay ningún país que esté libre de este flagelo. La diferencia está en los niveles de impunidad que pueden variar de un lugar a otro.

Obviamente, aun con una aprobación y observancia plena de preceptos éticos por parte del personal de inteligencia, probablemente siempre quedará un espacio imposible de controlar por completo en el comportamiento individual de los actores. Pero una cosa completamente distinta son las transgresiones consentidas u ordenadas por la autoridad política, tales como la persecución o espionaje de individuos u organizaciones incómodas en el propio país, sean éstos políticos de oposición, periodistas, jueces, líderes ambientalistas, entre muchos otros posibles. Estas transgresiones son, sin duda, mucho más graves, y las sociedades deben combatirlas estableciendo mecanismos eficientes para evitar su ocurrencia.

## Gestión de Inteligencia en las Américas

Frente a esta realidad y luego de analizar la discusión académica sobre el particular, cabe preguntarse si es necesario optar por la adopción de un código de ética profesional en las organizaciones de inteligencia o, por el contrario, basta con un poderoso y eficiente sistema de controles externos para evitar las contravenciones éticas y excesos de comportamiento.

Probablemente, lo óptimo será la utilización de ambos criterios, es decir, introducir normas de ética profesional como las descritas en el texto, tanto en códigos que puedan adoptar los propios servicios de inteligencia, y reforzar la formulación de recomendaciones emanadas de organizaciones internacionales como los casos del Consejo de Europa ya citado o de la Organización de Estados Americanos.

Un segundo elemento que se planteó en la discusión académica es el importante papel que juega el *ethos* profesional. Este fenómeno muy especial que declara quiénes somos debe surgir en el seno de las organizaciones de inteligencia, comprueba el valor del concepto para la práctica profesional. Esto se consigue y se refuerza no sólo con un proceso de introspección como se señaló más arriba, sino que también mediante un trato justo, basado en el mérito profesional de individuos, que a su turno implica un desarrollo formativo que se inicia con una selección rigurosa del personal, una carrera funcionaria predecible desde el ingreso hasta el término de funciones, una política de incentivos, el perfeccionamiento profesional continuo, unos reglamentos precisos y rigurosos sobre las diversas funciones y etapas de la carrera, entre otras muchas medidas.

Hasta hoy no existe un código universal sobre inteligencia ni nada parecido. Asimismo, el ejemplo español que se presentó, demuestra que no es un tema fácil de abordar porque despierta natural resistencia al interior de los servicios. Todavía no hay suficiente conciencia de que la ética y códigos deontológicos sólo van en beneficio de la profesión de inteligencia y en el mejoramiento de su imagen en la opinión pública. Es obvio que aquí hay un tremendo desafío por delante, que implicará una gran cuota de paciencia, sentido común y oportunidad de convencimiento mediante argumentos persuasivos.

Aquí comienza el muy importante rol que deben jugar legisladores y políticos. Por un lado, la legislación de inteligencia debe actualizarse allí donde no ha ocurrido todavía, incorporando todos los preceptos sobre protección de

los derechos humanos y de la privacidad de las personas. Esta legislación debe contener por cierto también las necesarias penas para quienes se vean tentados a cometer delitos y excesos que impliquen romper normas éticas profesionales mínimas y universalmente consensuadas.

Por otro, hay que apelar también a la responsabilidad de los políticos. Todo servicio de inteligencia, tanto aquellos que operan dentro del país como los que tienen como misión actuar en el extranjero, deben contar con la tutela y el direccionamiento del poder político. Éste es un papel de doble carácter. Por un lado, el poder político debe proteger a los organismos entregándoles misiones claras y definidas para desempeñar en la forma más eficiente posible y, al mismo tiempo, éste debe actuar en la forma más enérgica previniendo cualquier comportamiento reprochable, dando directrices claras sobre los límites éticos que no se deben traspasar. De ese modo explícito, los servicios no tendrán la dura tarea de decidir por sí mismos hasta dónde llegar en su cometido. Por cierto, el poder político de vez en cuando se cuidará de manipular el trabajo de las agencias de inteligencia para sus propios fines, muchas veces ajenos al bien común del Estado y la sociedad, lo cual sólo se puede ajustar por el electorado.

También es de la mayor importancia el rol que juegan los políticos en la designación de directivos y jefes de los servicios de inteligencia. No basta que los elegidos sean expertos en temas de seguridad, diplomacia, terrorismo y otros temas semejantes, sino que tengan una estatura moral intachable, pues su liderazgo será la medida para el desempeño profesional de sus subalternos.

En un país con una sociedad civil realmente empoderada y vigilante de sus derechos, tanto la prensa independiente como organismos de diverso tipo de esa misma sociedad civil organizada tienen un gran papel que jugar en el escrutinio de políticos y servicios de inteligencia. No es casualidad que la mayoría de las crisis en inteligencia que han terminado en reformas o nuevas legislaciones, se hayan originado en la denuncia de periodistas y otros actores sociales.

Por último, los propios servicios de inteligencia pueden desempeñar un papel mucho más activo si quieren mejorar su imagen y cumplir uno de los mandatos más exigidos por la sociedad actual, ser responsables y rendir cuentas periódicamente; lo que el mundo anglosajón denomina *accountability*. Para

## Gestión de Inteligencia en las Américas

ello existe una amplia gama de posibilidades, desde la cuenta anual que la mayoría de las agencias deben rendir por sus operaciones y gastos presupuestarios frente a los organismos de control parlamentario y gubernamental, hasta la proyección de su imagen institucional hacia la comunidad mediante páginas web y otros medios de difusión.

Resumiendo, se puede afirmar que el papel de la ética está tomando cada vez mayor importancia en el trabajo cotidiano de las agencias de inteligencia en todo el mundo. Hay esfuerzos en muchos lugares para inculcar la noción de que toda profesión, también la de analistas y operativos de inteligencia, debe guiarse por principios éticos sólidamente fundados que deben ser respetados a cabalidad. Cada país deberá escoger su camino. En algunos se redactarán códigos de ética en inteligencia; en otros, bastará con decálogos y recomendaciones escrupulosas y firmes. Pero sólo de ese modo, esta actividad tantas veces cuestionada, tendrá respetabilidad y legitimidad en un mundo plagado de incertidumbre.

### Biografía del autor

**Carlos Maldonado Prieto**, chileno, es licenciado en historia por la Martin-Luther-Universität, Halle, Alemania, y posee una maestría en Política de Defensa de la Academia de Guerra del Ejército de Chile. Ha sido socio académico del Instituto de Cooperación para la Seguridad Hemisférica (WHINSEC) y ha participado en cursos y seminarios organizados por el Centro Hemisférico de Estudios de Defensa (CHDS), ambos en Estados Unidos. Ha escrito los libros *El Prusianismo en las fuerzas armadas chilenas: Un estudio histórico, 1885-1945* (Santiago: Documentas, 1988) y *La Milicia Republicana: Historia de un ejército civil en Chile, 1932-1936* (Santiago: Servicio Universitario Mundial, 1988). También ha publicado artículos sobre inteligencia, historia de las fuerzas armadas, servicio militar y cuestiones policiales en revistas de Alemania, Canadá, Chile, Estados Unidos, Japón, Perú y Suecia, entre otros países. Correo: cmaldona99@gmail.com.





## Derechos Humanos y Ética de la Inteligencia: Análisis de Casos Cinematográficos

Moira Nakousi Salas

y

Daniel Soto Muñoz

### Inteligencia y Estado de Derecho

La configuración del Estado de Derecho en Latinoamérica comenzó a principios del siglo XIX coetáneamente con el proceso emancipador. Las nuevas repúblicas adoptaron, desde sus orígenes, la filosofía del liberalismo europeo y establecieron límites al ejercicio del poder público. Si bien el Estado antropomórfico concentró la capacidad soberana, sin consulta pública, de tomar decisiones y de emitir mandatos obligatorios dentro de su territorio,<sup>249</sup> al mismo tiempo, definió límites legales para su propia actuación. La principal restricción fue impuesta por la obligación de respetar los derechos de la personas.<sup>250</sup>

En el poder ejecutivo quedó radicada la administración de los bienes comunes y la ejecución de las funciones básicas para la supervivencia de la colectividad. El monopolio de la fuerza física legítima se convirtió en una función auxiliar de los gobernantes. La fuerza es, desde entonces, el último recurso para asegurar la obediencia ciudadana a las normas jurídicas y una garantía de seguridad frente a las amenazas internas y externas.<sup>251</sup>

Desde el origen del Estado moderno, la principal preocupación de los gobernantes ha sido el ejercicio de la soberanía y, en esa aplicación, la mantención del equilibrio entre seguridad y libertad. En casi todo el siglo XX, la seguridad estuvo vinculada al mantenimiento de la integridad del Estado, hasta el surgimiento, a fines de los años 90, de los conceptos de “seguridad humana” y “seguridad multidimensional”, que trasladaron el foco de interés hacia las personas.<sup>252</sup> En esta evolución, muchas veces las violaciones sistemáticas a los derechos humanos fueron justificadas como un mal menor en favor de la seguridad del Estado.

La película “*Unthinkable*” o “El día del juicio final”, el foco de este ensayo, presenta con crudeza el conflicto de intereses que plantean las políticas públicas de seguridad y, dentro de ellas, el papel de los sistemas de inteligencia

en democracia: la eficacia en la prevención y represión de amenazas, versus el costo social que significa la restricción de los derechos y las libertades.<sup>253</sup> El filme plantea una situación extrema y se centra en la discusión sobre la posible justificación de actos de la autoridad que potencialmente podrían beneficiar a toda la comunidad pero que implicarían suprimir los derechos más elementales de algunas personas. El director, no obstante, pone desde el principio al espectador del lado de las potenciales víctimas inocentes y, con ello, reduce la posibilidad de ofrecer perspectivas claras sobre el verdadero reto de la inteligencia en un Estado de Derecho: garantizar la seguridad sin mermar la libertad.<sup>254</sup> En el presente trabajo, entretanto, se investigan las opciones inevitables que enfrentan los profesionales de inteligencia en un Estado de Derecho.

La comprensión de la seguridad como un medio para conseguir el bien común eleva el concepto “securitario” a una dimensión democrática dentro de un Estado de Derecho. Los derechos más importantes de las personas son el derecho a la vida y a la libertad de acción. La seguridad, por tanto, ocupa un rol secundario y es un mero instrumento para garantizar ambos derechos.<sup>255</sup> Cada régimen político elabora su propio concepto a partir de este equilibrio y así define el modelo de sus agencias de inteligencia. Mientras en los regímenes democráticos, por definición, la inteligencia sirve precisamente para afirmar la libertad de las personas, en los regímenes totalitarios, y autoritarios, la seguridad se convierte en una ideología que pone a las agencias de inteligencia al servicio de los intereses del poder restringiendo la libertad de la gente.

Además, en el Estado de Derecho, todas las instituciones están bajo los límites y controles que el ordenamiento jurídico establece, incluidas las agencias de inteligencia. Éstas se dirigen principalmente a prevenir amenazas que puedan afectar a la seguridad y la defensa y no tienen capacidad decisoria en la conducción del Estado. No obstante, en las dictaduras ideológicas (totalitarismos) o burocráticas (autoritarismos), y a veces incluso bajo regímenes democráticos,<sup>256</sup> se promueve la idea de la existencia de “enemigos internos” que hay que descubrir y castigar. En estos casos, son los servicios secretos los encargados de reprimir la posible disidencia.<sup>257</sup> Una interesante paradoja se produce con la transformación de los servicios secretos de regímenes no democráticos que siguen funcionando depuestos los autoritarismos.

El cine ofrece interesantes ejemplos de estos tres modelos de gobierno y sus respectivas éticas públicas. La película “La vida de los otros” (*Das Leben der*

## Gestión de Inteligencia en las Américas

*Anderen*”) de Florian Henckel von Donnersmarck (2006) expone la implacable y persistente violación al derecho a la intimidad practicada por la *Stasi* contra los disidentes del régimen comunista en la República Democrática Alemana.<sup>258</sup> El filme argentino “El secreto de sus ojos” de Juan José Campanella (2009) trata sobre la impunidad de un criminal común que se integra a una agencia de seguridad del régimen militar de turno.<sup>259</sup> “Quémese después de leerse” (*Burn after reading*) de los hermanos Coen (2008) es una irreverente comedia que narra el traumático proceso de jubilación de Osborne Cox quien se ve forzado a dejar una larga carrera de analista en una importante agencia de inteligencia en la cual ha estado sujeto a diversos tipos de controles <sup>260</sup> (ver Tabla 5).

Tabla 5 Tipología sobre Formas de Gobierno y Agencias de Inteligencia		
GOBIERNO	TIPO DE AGENCIA	EJEMPLOS EN PELÍCULAS
TOTALITARISMO	Policía política	“La vida de los otros” de F. von Donnersmarck (2006)
AUTORITARISMO	Agencia de seguridad independiente	“El secreto de sus ojos” de J.J. Campanella (2009)
ESTADO DE DERECHO	Sistema de inteligencia	“Quémese después de leerse” de los hermanos Coen (2008)

**Fuente:** Elaboración propia de los autores (2012) a partir de González, Larriba y Fernández, “Servicios de Inteligencia y Estado de Derecho”, en José Luis González Cussac, coord., *Inteligencia* (Valencia, Tirant Lo Blanch, 2012), pp. 284-287.

### Presentación del caso: la película *Unthinkable* o *El día del juicio final*

**La Escena:** Se encuentra detenida una persona que afirma haber instalado tres artefactos nucleares en diversas zonas urbanas del país. Según ha expresado en un video las tres bombas estallarán simultáneamente en cuatro días más. Las autoridades han calculado que el material atómico empleado en los dispositivos sería capaz de causar entre seis y diez millones de muertes. El cautivo se niega a ofrecer voluntariamente la información que permitiría desactivar los explosivos o evacuar a las posibles víctimas. ¿Se justifica moral y jurídicamente la posibilidad de torturar al autor de este posible atentado para salvar la vida de millones de personas? Esta es la controversia que presenta la película “*Unthinkable*” o “El día del juicio final” de Gregor Jordan (2009) y así se presenta el problema central que se analizará en este artículo.<sup>261</sup>

## Inteligencia y derechos humanos

Tomando en cuenta el escenario planteado arriba: Los canales de televisión anuncian la búsqueda de un delincuente prófugo acusado de asesinar a un policía y de secuestrar a dos niños. Se encarga a la población dar cuenta del paradero del hombre de la fotografía, y de la ubicación de tres lugares que también se muestran en la pantalla. La unidad de contraterrorismo del FBI de Los Ángeles comienza la misma indagación, pero con una motivación distinta a la informada en la transmisión. La agente Helen Brody recibe la orden de pesquisar a un centenar de sospechosos posiblemente vinculados al hombre de las noticias. La orden viene del poder central. Se dispone personal de apoyo del mismo FBI y de las policías locales para detener a estas personas. Se trata de integrantes de supuestas células terroristas islámicas radicados en los Estados Unidos.

Todos los servicios secretos cuentan con alguna tipo de autoridad para aplicar medidas que restringen o afectan, de una u otra manera, algunos derechos y garantías fundamentales de las personas. La mayoría de las agencias puede, por ejemplo, efectuar seguimientos y vigilancias, implementar medidas intrusivas que afecten las comunicaciones y emplear agentes encubiertos e informantes. Aquellos servicios secretos que efectivamente cuentan con potestades policiales pueden, adicionalmente, ingresar a lugares cerrados y efectuar registros en ellos, así como registrar personas, vehículos y equipajes, y, eventualmente también, privar de libertad a quienes representan una amenaza.

El Estado de Derecho impone que estas atribuciones se efectúen de manera excepcional y bajo ciertas condiciones, y sujetas a controles, ya sea del poder ejecutivo, el legislativo o el judicial. Atendiendo la necesidad de control externo en la mayoría de los sistemas de inteligencia estos procedimientos especiales los ejecutan las policías bajo la supervisión judicial. Como complemento los agentes deben guardar secreto de su cometido, de sus resultados y de las informaciones que lleguen a su conocimiento en ese desempeño.

Los sistemas de inteligencia Latinoamericanos están estructurados por legislaciones que explícitamente establecen la finalidad de preservar el orden constitucional. Estas leyes, además, les exigen a los organismos de inteligencia adecuar sus métodos de búsqueda de información a las exigencias constitucionales y legales. Todas estas normas hacen referencias imperativas a la obligación de respetar los derechos humanos (ver Tabla 6).

## Gestión de Inteligencia en las Américas

Tabla 6 Referencias a los Derechos Humanos en las Leyes de Inteligencia Latinoamericanas				
ESTADO	LEY DE INTELIGENCIA	ARTÍCULOS	CONSTITUCIÓN VIGENTE	ARTÍCULOS
ARGENTINA	25.520 de 2001	3, 4 y 5	1994	8,14,15, 18,20, 33, 75 No.22, 23, 24, 86
BRASIL	9.883 de 1999	1.1	1998	1, 4.II, 5.XLI, LXXVII.1, 17
CHILE	19.974 de 2004	3, 4 y 34.c	1980	1, 5 inciso 2, 19.
COLOMBIA	195 de 2011	2, 4, 14, 15 y 24	1991	11-41, 91-95, 118, 164, 214, 222, 277, 282
ECUADOR	Ley Registro Oficial N°35 de 2009	4, 19, 23, 30 y 33	2008	10, 11, 18, 27 41, 51, 57, 58, 66, 83, 93, 156, 158, 163, 171, 384, 398, 416, 417, 423, 424, 426, 428, 436
MÉXICO	Ley de Seguridad Nacional de 2005	25 y 31	1917	2.A.II, 2.B.VIII, 21, 102.B
PERÚ	28.664 de 2005	3 y 4	1993	1-3, 14, 44
VENEZUELA	Ley Gaceta Oficial 38.940 de 2008	10 y 24	1999	1-3,19-31, 46, 55, 76, 132, 152, 261, 271, 272, 278, 280, 281, 326, 337, 339, 350

**Fuente:** Elaboración propia de los autores (2012).

Para evitar la posible colisión entre los intereses del Estado con los de las personas, las tareas intrusivas de los servicios de inteligencia deben sujetarse a las condiciones de legitimidad que imponen, tanto el ordenamiento jurídico interno, como el derecho internacional de los derechos humanos. No basta con que los sistemas de inteligencia estatales sean creados por una ley, sino que es necesario que sus actividades se adecuen también a la norma legal.<sup>262</sup> Sólo el

respeto al principio de legalidad permitirá que los resultados de las agencias de inteligencia sean efectivamente útiles a la gestión estratégica del Estado.

En la práctica, las normas internacionales ajustables a la actividad de inteligencia y contrainteligencia son las mismas que regulan las investigaciones policiales.<sup>263</sup> Algunos casos de ficción útiles para ilustrar su aplicación se pueden encontrar en las películas que se mencionan a continuación y que se esquematizan en la tabla 7. Éste resume los posibles conflictos de intereses que pueden presentar los procedimientos especiales de obtención de información con el derecho internacional de los derechos humanos.

### *Seguimientos y vigilancias*

Los seguimientos consisten en maniobras físicas o tecnológicas, presenciales o a distancia, que permiten mantener un blanco previamente seleccionado bajo observación continua. Las vigilancias son rastreos de igual naturaleza que se ejecutan de manera más estática.

En la práctica, mientras el blanco circula por espacios públicos, y éste no advierte que está siendo examinado, no sufre una perturbación aparente en el ejercicio de sus derechos. No obstante, la posibilidad que el Estado pudiese estar observando a las personas continuamente y almacenando esta información afecta, en el fondo, la seguridad jurídica de las personas. Esta incertidumbre es mayor si la actividad estatal pueda afectar la esfera privada o íntima. Una inseguridad de este tipo dañaría la garantía de predictibilidad de la actividad estatal.

La observación ininterrumpida de las actividades cotidianas de los ciudadanos puede generar una limitación psicológica que impida el libre ejercicio de los derechos de circulación, una perturbación al derecho de asociación,<sup>265</sup> y podría afectar incluso la presunción de inocencia, revirtiendo la carga de la prueba frente a eventuales imputaciones delictivas.<sup>266</sup>

La película “Contacto en Francia” (*The French Connection*) muestra el extenso seguimiento que efectúa el implacable policía Jimmy “Popeye” Doyle a los integrantes de “la conexión francesa”, liderada por el criminal francés Alain Charnier. La persecución se efectúa, con técnicas y resultados dispares, y se extiende por toda la ciudad para descubrir la participación criminal de los diversos personajes de la trama.<sup>267</sup>

## Gestión de Inteligencia en las Américas

### *Medidas intrusivas en las comunicaciones*

En la actualidad las intervenciones o interceptaciones de las comunicaciones pueden extenderse a la apropiación de correspondencia postal, la intervención telefónica o de sistemas y redes informáticas, a las escuchas y la grabación telemática.

El problema más delicado que pueden generar estas medidas intrusivas, es, nuevamente, la posibilidad de la injerencia arbitraria del Estado en la privacidad e intimidad de las personas. Se debe considerar que el derecho a la intimidad importa la obligación del Estado de tutelar la confidencialidad, o inviolabilidad del hogar, proteger las comunicaciones y las relaciones familiares, y el derecho de las personas a desarrollar su personalidad.<sup>268</sup>

Por eso tenemos en nivel internacional el “Código de conducta para funcionarios encargados de hacer cumplir la ley” de 1979.<sup>269</sup> Su artículo 4 impone, también a los agentes de inteligencia la obligación de proteger la intimidad: “las cuestiones de carácter confidencial de que tengan conocimiento los funcionarios encargados de hacer cumplir la ley se mantendrán en secreto, a menos que el cumplimiento del deber o las necesidades de la justicia exijan estrictamente lo contrario”.

En el filme “La vida de los otros” (*Das Leben der Anderen*), un corrupto ministro de República Democrática Alemana dispone que la *Stasi* intervenga y grabe cada una de las comunicaciones privadas, e incluso íntimas, que un dramaturgo disidente sostiene en el interior de su casa. Las motivaciones del ministro Hempf no son estrictamente políticas y termina afectando de forma dramática la vida pública y privada del escritor Georg Dreyman y su novia la actriz Christa María Sieland.

### *Agentes encubiertos, infiltrados e informantes*

Los agentes encubiertos son funcionarios que ocultan su identidad oficial con el fin de obtener información para el proceso de inteligencia. Eventualmente, éstos pueden introducirse en organizaciones criminales o terroristas de modo clandestino, y reciben el nombre de “agentes infiltrados”. Los informantes, también llamados informadores, por su parte, son personas que no pertenecen a los servicios de inteligencia y suministran antecedentes, normalmente, a cambio de retribuciones.



Los problemas comunes que presentan estos tres tipos de actores (agentes encubiertos, infiltrados e informantes) derivan de sus identidades secretas. Esto dificulta tanto la validez de los medios de prueba que puedan conseguir como la posibilidad de defensa de los imputados, quienes por ejemplo, no tienen la posibilidad de examinar los testigos anónimos. Desde ambas perspectivas, este secretismo afecta las garantías del debido proceso de ley.<sup>270</sup>

El empleo de informantes presenta además algunos problemas éticos importantes. A menudo están estrechamente vinculados a la delincuencia, actúan motivados por la protección que les da el Estado, y los contactos que mantienen con los agentes son secretos. Este proceso puede ser riesgoso para el sistema porque los informantes pueden aprovechar sus contactos para cometer delitos en la impunidad, o pueden alentar a otros a cometer delitos para recibir dinero a cambio de esa misma información. Por otra parte, la reserva y el manejo de dineros pueden incentivar la corrupción.<sup>271</sup>

“Los Infiltrados” (*The Departed*) de Martin Scorsese (2006), no es una película que recaerá estrictamente sobre servicios de inteligencia, pero presenta interesantes personajes y situaciones relacionadas con agentes encubiertos, infiltrados e -inesperados- informantes. El policía William “Billy” Costigan Jr. se introduce en la organización criminal de Francis “Frank” Costello. Al mismo tiempo que trabaja para revelar la estructura y operaciones de esta organización mafiosa, debe identificar un “topo” que ha sido incrustado en la Unidad de Investigaciones Especiales.<sup>272</sup>

### *Entrada y registro en lugares cerrados y registro de personas*

La entrada y registro en lugares cerrados, también conocido como “registro de morada” o “registro domiciliario”, busca información para el proceso de inteligencia. Se practica evidentemente, en lugares en los que el propietario no tiene intención de facilitar voluntariamente la exploración y afecta, esencialmente, el derecho de inviolabilidad del domicilio.<sup>273</sup> Este derecho, además, está concebido como una garantía del debido proceso para evitar la recolección ilegal de pruebas incriminatorias.<sup>274</sup>

El registro de personas, vehículos o equipaje, también denominado “requisa”, es una medida invasiva, que se practica directamente sobre el afectado, para encontrar objetos que puedan proporcionar datos útiles a una investigación.

## Gestión de Inteligencia en las Américas

Los derechos y garantías en juego son los mismos del caso anterior. Dos condiciones importante para su ejecución son que el sexo del agente que lo practica debe ser el mismo que el del afectado,<sup>275</sup> y que se efectúen en privado para minimizar la afectación de la dignidad y el decoro de la persona fiscalizada.<sup>276</sup>

El caso que presenta “La Ciudad de las Tormentas” (“*The Green Zone*”) de Paul Greengrass (2010)<sup>277</sup> introduce la actividad de inteligencia en un conflicto armado y expone los trances de la aplicación del derecho en una zona de ocupación. El filme ejemplifica la forma como la calidad de la inteligencia puede influir decididamente en el diseño e implementación de operaciones militares y policiales. En la historia, la mayoría de los procedimientos especiales de obtención de información son ejecutados por militares. Esboza que los resultados de estas maniobras pueden ser nefastos cuando se confunde el régimen jurídico aplicable para el uso de la fuerza y no se distingue correctamente entre “*law enforcement*” -dentro del ámbito nítidamente de los derechos humanos, con “*conduct of hostilities*” -bajo la esfera del derecho internacional humanitario.

### *Privación de libertad*

Existen distintas formas de privación de libertad legítimas practicadas por la autoridad. Estas incluyen la detención por delito flagrante (comúnmente denominado arresto), la detención por orden judicial o por disposición de la autoridad administrativa, la reclusión por sentencia judicial, la institucionalización por razones de salud, o la internación por motivos cautelares. La privación de libertad puede efectuarse en establecimientos públicos o privados, y su principal característica es el sometimiento de una persona a un régimen de privación de su autonomía ambulatoria.

Todos los tipos y casos de privación de libertad, incluyendo los que pudieran practicar agentes de inteligencia de policía, están sujetos a la obligación de respeto al derecho a la integridad personal y el trato humano.<sup>278</sup> Las garantías más importantes, en este sentido son las que aseguran la indemnidad de la persona inmediatamente después de haberse practicado su aprehensión material: el detenido tiene el derecho de conocer las razones de su detención, ser llevado sin demora ante un juez, y ser juzgado dentro de un plazo razonable.<sup>279</sup> Posteriormente, mientras dura su cautiverio, se debe garantizar un trato humano y el respeto a la dignidad inherente a todo ser humano.<sup>280</sup>

Los principios anteriores excluyen la posibilidad de que una persona reciba “legítimamente” tortura física o moral o sea expuesto a técnicas de interrogación inhumanas o degradantes.

El conflicto más serio con los derechos humanos, se da en las detenciones “preventivas” y en la práctica de interrogatorios abusivos contra sospechosos de participación en organizaciones terroristas. La película “La Batalla de Argelia” (“*La Battaglia di Algeri*”) de Gillo Pontecorvo (1966) recrea las operaciones de contrainteligencia efectuadas por Francia en la guerra de liberación argelina. El Coronel Mathieu comienza restringiendo la libertad de desplazamiento de la población argelina y, luego, dispone detenciones aleatorias para implementar brutales técnicas de interrogación que permitan develar las cúpulas del Frente de Liberación Nacional.<sup>281</sup>

Tabla 7 Fuentes de Controversias entre la Actividad de Inteligencia y Protección de los Derechos Humanos Ejemplificadas en Determinadas Películas			
ACTIVIDAD DE INTELIGENCIA	CONTROVER-SIA JURÍDICA	NORMAS EN CONFLICTO	EJEMPLOS EN PELÍCULAS
SEGUIMIENTOS Y VIGILANCIAS	Presunción de inocencia	Declaración Universal (art.11), Pacto Internacional de Derechos Civiles y Políticos (PIDCP) (art.14), Convención Americana (art.8)	“Contacto en Francia” de W. Friedkin (1971)
MEDIDAS INTRUSIVAS EN LAS COMUNICACIONES	Derecho a la intimidad, honra y dignidad	Declaración Universal (art.12), Convención Americana (art.11)	“La vida de los otros” de F. von Donnersmarck (2006)
AGENTES ENCUBIERTOS, INFILTRADOS E INFORMANTES	Derecho a examinar a los testigos	Declaración Universal (art.10), PIDCP (art.14), Convención Americana (art.8)	“Los Infiltrados” de M. Scorsese (2006)

Tabla 7, (continua)			
Fuentes de Controversias entre la Actividad de Inteligencia y Protección de los Derechos Humanos Ejemplificadas en Determinadas Películas			
ACTIVIDAD DE INTELIGENCIA	CONTROVER-SIA JURÍDICA	NORMAS EN CONFLICTO	EJEMPLOS EN PELÍCULAS
ENTRADA Y REGISTRO EN LUGARES CERRADOS Y REGISTRO DE PERSONAS	Derecho a la libertad y seguridad personales	Declaración Universal (arts 3 y 11.2), PIDCP (arts. 9, 11, 14 y 15), Convención Americana (arts. 5, 7, 9 y 10)	"La Ciudad de las Tormentas" de P. Green-grass (2010)
PRIVACIÓN DE LIBERTAD	Integridad personal y trato humano	Declaración Universal (art.5), PIDCP (art.5), Convención Americana (art.5), Conven-ción contra la Tortura, Conjunto de Principios para Protección de Per-sonas Detenidas	"La batalla de Argelia" de G. Pontecorvo (1966)

Fuente: elaboración propia de los autores (2012)

### Análisis de caso cinematográfico: película *El día del juicio final*

Sólo es posible un "examen de conformidad" parcial de las actuaciones de las agencias de "*Unthinkable*" con los estándares internacionales. La película no se detiene en razonar jurídicamente los procedimientos, sino que los plantea, y justifica, como cuestiones normales ante una situación de emergencia nacional:

- a) Al comienzo de la película el agente Phillips muestra a Helen Brody un expediente, hecho llegar por error, desde la CIA al FBI. En él aparece una fotografía de Humphries (un desconocido) tomada en una vigilancia ilegal. Se debe recordar que la CIA no tiene competencia para recolectar información de inteligencia relacionada con

ciudadanos estadounidenses, dado que, su misión es obtener información de la inteligencia y contrainteligencia extranjera.<sup>282</sup>

- b) A continuación, el mismo Phillips junto a un compañero irrumpe, sin autorización judicial, en la casa de Humphries y, tras el fracaso de esta primera intervención, entran otros dos agentes que rescatan a los primeros, detienen a Humphries y registran su morada.
- c) El FBI declara que cuenta con información de 80 personas que estarían vinculadas, de una u otra manera, en actividades terroristas. Todos estos datos han sido obtenidos presumiblemente desde fuentes cerradas, pero se ignora la legalidad del proceso. Respecto de todos estos sospechosos se ordena sin más: “debemos interrogar a sus familias, sus amigos, sus compañeros de trabajo, cada potencial vínculo terrorista que hayan estado rastreando durante los últimos nueve meses y debemos hacerlo ahora mismo”. Estas detenciones masivas serían ilegales y arbitrarias.
- d) Paralelamente, el presunto terrorista, Younger-Yusuf se encuentra privado de libertad en un lugar secreto. No se le han dado a conocer hasta ahora las justificaciones legales de su detención, pues fue aprehendido por su actitud “sospechosa” y es mantenido allí tras haber afirmado que puso tres bombas de destrucción masiva. El motivo no declarado de la detención sería, entonces la autoinculpación. El detenido no ha sido llevado ante un juez y no existe intención de parte de sus captores de que éste sea juzgado por algún delito dentro de un plazo razonable. Es decir, en la detención de este presunto terrorista no se han cumplido ninguna de las obligaciones internacionales mínimas.

### *Inteligencia y tortura*

La escena: Steven Arthur Younger, alias Yusuf Atta Mohamed, se encuentra detenido desde hace 24 horas. Como sabemos, se entregó voluntariamente a la policía local y tras su aprehensión ha afirmado que instaló tres artefactos nucleares. Nadie lo vio instalándolos, ni nadie sabe tampoco donde podrían ubicarse. Contrainteligencia ha confirmado su participación en la adquisición de material radiactivo años atrás y ha ratificado que cuenta con cono-

## Gestión de Inteligencia en las Américas

cimientos y experiencia en desactivación de bombas y armas nucleares. Las fuerzas armadas tienen el control de la situación, porque, legalmente están facultadas para actuar en casos de emergencia nacional con el fin de “reprimir cualquier insurrección, asociación ilícita o conspiración”. Hasta el momento, Younger-Yusuf ha sido objeto de apremios autorizados: “no ha sido golpeado pero ha sido expuesto al calor, el frío, la privación de sueño, el ruido, las luces brillantes, y a las amenazas de violencia”. Un representante del gobierno da instrucciones a una persona enviada por una agencia de inteligencia de defensa. Henry Harold Humpries, alias “H”, es el experto que aplicará tormentos al detenido para que proporcione la información que permita salvar la vida de millones de personas.

En general se entiende por tortura cualquier acto mediante el cual se aplica intencionalmente dolor o sufrimientos graves, físicos o psicológicos a una persona.<sup>283</sup> Su uso repugna al pensamiento moderno<sup>284</sup> y se encuentra expresamente prohibida tanto por el derecho internacional, como por la totalidad de los ordenamientos penales. No obstante, existe una tendencia reciente que plantea la posibilidad de su justificación moral y jurídica en casos en que infringir daños a unos pocos puede servir para beneficiar a muchos. Este es el argumento de la película “*Unthinkable*”, que desarrolla el ya clásico caso de la “bomba de relojería” también denominado “*Ticking Time-Bomb Scenario*”.<sup>285</sup>

Las premisas fácticas sobre las que se sostiene el caso son las siguientes: se ha instalado un dispositivo automático en un lugar desconocido, éste causará incuantificables víctimas, el autor se encuentra detenido pero se niega a proporcionar la información. La conclusión de estas premisas sugiere como en la película que estaría justificado torturar al detenido para obtener esta información que salvará la vida de inocentes. Como consecuencia los partidarios de la tortura proponen regularla jurídicamente para evitar un uso indiscriminado y sin control.

Estas premisas, no obstante, son totalmente refutables.

La primera objeción al escenario de la bomba es su construcción artificiosa. Sólo sabríamos que la persona detenida puso una bomba si la vimos instalándola. En ese caso no habría que interrogarlo para conocer su ubicación. En “*Unthinkable*”, se detiene a alguien que se culpa asimismo, que da detalles filmados de sus preparativos, y que luego, guarda silencio durante los primeros días de su cautiverio. Inaudito. En la práctica si se aceptara este argumento

se debiesen detener cotidianamente decenas de personas sospechosas y quizás tras cientos de “asépticos” maltratos se podría detectar un explosivo.

La segunda objeción es que en este ejercicio se olvida que no hay torturas benéficas que puedan admitir una graduación “aceptable” de tratos vejatorios. La violencia siempre tiene efectos dañinos para quien la recibe, para quien la ejerce y para quien la presencia.

La tercera objeción es que la información obtenida mediante tormentos es de mala calidad y no se puede conseguir en un breve lapso. Los casos en los que se promueve su uso están normalmente urgidos por una amenaza inminente. La excepción al escenario normal de la bomba es el de “*Unthinkable*”, que da cuatro largos días para emplear todo tipo de técnicas de interrogatorio contra el sospechoso que incluyen el ahogamiento con una bolsa plástica, castración, golpes de bastón, prolongadas sesiones de colgaduras, electricidad, extracción de uñas, manos clavadas con un punzón, “*spray*” irritante en los oídos, extracción de muelas sin anestesia, inmersión temporal en agua, la observación de un homicidio y la amenaza de un grave mal a los propios hijos. Todo esto matizado con la sonata para piano Opus 13 “*Patética*” de Beethoven y algunos masajes proporcionados por la agente Helen Brody al imperturbable Younger-Yusuf.

El caso del escenario de la bomba se vincula a la inteligencia porque equivocadamente se asocia la tortura con las técnicas de interrogatorio. Esto resulta profundamente erróneo. Primero, porque los servicios de inteligencia, en general, no tienen facultades de policía; y, segundo, porque en un Estado de Derecho los órganos estatales deben adecuar sus métodos a la ley y la tortura se encuentra tipificada como un delito.

La tortura no es, ni puede ser, una práctica válida para la búsqueda de información en “fuentes cerradas”. La barbarie no es una herramienta de la inteligencia y sólo puede vincularse a agencias espurias bajo sistemas políticos dictatoriales. Un autor chileno cuya obra generó controversia<sup>286</sup> ha sostenido, con razón, que “la guerra sucia no forma parte de las actividades que por doctrina debe desarrollar la inteligencia”.<sup>287</sup> Agrega que una de las características de la guerra sucia fue la institucionalización de la tortura dado el desprecio de la doctrina de la seguridad nacional por la vida y la dignidad de las personas. Señala, además, que la tortura, independientemente del

## Gestión de Inteligencia en las Américas

método que aplique, es siempre un acto cruel sin justificación ética y que respeto de principios humanos (vida y dignidad) permite “distinguir a un delincuente de una persona honrada”. El razonamiento de Palamara es sencillo y concluyente.

### *Gestión de la inteligencia*

La Escena: La actuación de Younger-Yusuf genera en sus captores una sensación de desconfianza generalizada, junto a angustiantes sentimientos de vulnerabilidad e indefensión. El sistema de inteligencia estatal ha sido completamente burlado: por un lado, el FBI cuenta con un equipo especializado que no logró descubrir la conexión que podía existir entre el detenido y agrupaciones terroristas dentro del país; por otro, ni la CIA, ni otras agencias de la comunidad de inteligencia, fueron capaces de detectar que un ex funcionario militar había dejado las filas con un profundo resentimiento, y que luego se había vinculado con inteligencias hostiles. En este escenario de fracasos e incertidumbres, se encarga a Henry Harold Humpries, alias “H”, que emplee tormentos contra el detenido para obtener la información que confirme la existencia de las bombas y permita su ubicación.

### *Identidades únicas*

El origen de la tortura genera una interrogante importante. ¿En qué momento y qué tipo de personas son las que toman una decisión tan fría y calculada como la de infligir dolor inhumano a otra? En otras palabras cómo es posible que grupos de personas, organizaciones y aparatos estatales, puedan institucionalizar una práctica tan abominable como el castigo físico insufrible. Qué elementos subyacen en una decisión como ésta, y qué consideraciones hace quien ejecuta los tormentos para minimizar la importancia del dolor ajeno.

Uno de los mayores problemas que enfrenta la humanidad es la violencia perpetrada entre los mismos seres humanos. Son cientos de millones de víctimas a lo largo de la historia ocasionadas por las guerras, la agresión interpersonal, la tortura, y actos similares. Muchas de éstas se han explicado por motivaciones políticas, religiosas, étnicas o de género, y en otros casos sólo por la odiosidad entre grupos “enemigos”.<sup>288</sup> En general, es difícil comprender cómo se crean y diferencian estos grupos, conformados por hombres y mujeres que, por encima de cualquier otra consideración, son personas comunes y corrientes.



Categorizar es un proceso natural y automático en el ser humano. La función principal de la categorización es facilitar la comprensión de la complejidad de la información recibida. Este ejercicio permite la adaptación cognitiva y conductual.<sup>289</sup> Desde los primeros años de vida ordenamos y seleccionamos cosas, situaciones y personas. Todo agrupamiento, no obstante, conlleva una simplificación puesto que, al destacar los rasgos comunes, y como consecuencia, se acentúan las diferencias con los objetos separados.

En la categorización social existe también esta tendencia a exagerar las diferencias con las personas pertenecientes a categorías distintas, y, al mismo tiempo, a minimizar las que existen dentro de los integrantes de la misma. Surge, así, el “endogrupo” (“nosotros”) y el “exogrupo” (“los otros”). Dentro del endogrupo se crea una espontánea atracción y predisposición positiva hacia sus miembros, que Tajfel denomina “discriminación gratuita”.

En las primeras imágenes “*Unthinkable*”, se presenta al antagonista mientras graba, una y otra vez, el discurso en que revela la existencia de los dispositivos nucleares. Se lo identifica primero como una persona normal y nerviosa. Luego se conoce su verdadera identidad cuando revela su nombre árabe y expresa sus torcidas maquinaciones. A partir de entonces, el hombre joven y perturbado deja de ser parte del endogrupo y se convierte en una amenaza.

La “identidad social”, entendida como conciencia compartida de pertenecer a un mismo grupo o categoría social, ha sido definida como “parte del auto concepto de un individuo que deriva del conocimiento de su pertenencia a un grupo (o grupos) social junto con el significado valorativo y emocional asociado a dicha pertenencia”.<sup>290</sup> Se generan sentimientos de calidez, fortaleza, protección y orgullo. Se despliega un recurso -o “capital”- social que ayuda a desarrollar los compromisos de solidaridad y militancia que dan consistencia al grupo.<sup>291</sup>

Esta lealtad y favoritismo por el endogrupo, sin embargo, no constituyen antecedentes obligados de hostilidad hacia el exogrupo. La odiosidad surge cuando se percibe una amenaza (real o imaginada) a la integridad de esta identidad. En el concepto de los captores, Younger-Yusuf es una amenaza cierta, porque ya ha sido capaz de matar a más de 50 personas en un atentado explosivo inesperado, lo cual ha ocurrido después de su detención. Younger-Yusuf, por su parte, se presenta como un patriota, un hombre que está en la

## Gestión de Inteligencia en las Américas

posición de las personas religiosas y sometidas por el gobierno a la tortura hasta la muerte.<sup>292</sup> A juicio del detenido, en contraste, la autoridad gubernamental es también una amenaza permanente para el mundo islámico porque diariamente mata esa misma cantidad de gente inocente.

Las agencias de inteligencia gubernamentales de “*Unthinkable*” funcionan en equipos pequeños, bien adoctrinados y equipados. Todos portan identificaciones corporativas que lucen de manera vistosa y con orgullo (tanto así, que Helen Brody debe esforzarse por cuidar su vestimenta al cruzar la calle para no exhibir su arma de fuego). Lo mismo ocurre con los militares, quienes se muestran como depositarios de conocimientos insondables y ejecutores eficientes de las órdenes del poder central. Todos los discursos reafirman una pertenencia definida.

La ilusión de una identidad única o “afiliación singular”, hábilmente cultivada o débilmente reprimida, puede convertirse en un poderoso incentivo para violentar a los miembros de otro grupo y es el punto de partida de la persecución, la tortura y el exterminio.<sup>293</sup> De las desconfianzas y amenazas hacia el exogrupo -reales, imaginadas, o bien, intencionadamente introducidas- surge la figura del enemigo.<sup>294</sup> Éste, con sus intenciones siniestras, justifica todas las acciones en su contra y permite asentar la propia identidad (ver Tabla 8).

Tabla 8 Ideas que Alimentan las Identidades Únicas	
CAUSAS	TIPO DE AFILIACIÓN SINGULAR
SUPERIORIDAD DEL ENDOGRUPO	Etnocentrismo. Grupo elegido, privilegiado por la naturaleza, o llamado a una misión sublime.
SENTIMIENTO DE INJUSTICIA	Creencia en la existencia de agravios y humillaciones inaceptables, que afectan su territorio, derechos y libertades.
VULNERABILIDAD	Amenaza real o percibida de vulnerabilidad frente a otro grupo.
DESCONFIANZA	Del exogrupo sólo se pueden esperar desgracias. Puede ser paranoia colectiva o historia real de agravios sufridos.

Tabla 8 Ideas que Alimentan las Identidades Únicas	
CAUSAS	TIPO DE AFILIACIÓN SINGULAR
INDEFENSIÓN	Percepción colectiva de pérdida de control, dependencia y desamparo, que llevan a la insurgencia y confrontación.
FINES Y OBJETIVOS	La grandeza a la que está destinada el endogrupo, justifica cualquier medio.

**Fuente:** Elaboración de los autores, basada en Amalio Blanco Abarca, “La Condición de ‘Enemigo’: El Ocaso de la Inocencia,” en Manuel Cancio Melia y Laura Pozuelo Pérez, coords., *Política criminal en vanguardia: Inmigración clandestina, terrorismo, criminalidad organizada* (Navarra, España: Editorial Aranzadi SA, 2008), pp. 296 and 297.

Younger-Yusuf, a los ojos de sus captores, se encuentra en una categoría sospechosa: nació en Estados Unidos, pero creció en Islamabad y habla farsi y árabe. En el fondo, aunque sea estadounidense, pertenece a otro grupo, al mismo de las personas de las fotografías de la red elaborada por el FBI. Su foto, que estaba en un diario mural contiguo al del gráfico, es puesta junto a los sospechosos árabes. Torturar al detenido se convierte en una razón de Estado. Los captores quitan al detenido su nacionalidad y con ello su identidad de persona. Brody trata de refutar la legitimidad de practicar la tortura a un supuesto “combatiente ilegal” que, en el fondo, es un ciudadano estadounidense, pero una autoridad presente dictamina: “Así fue hasta ayer, ahora no tiene nacionalidad”.

### *Del recelo a la inhumanidad*

Albert Bandura afirma que “dadas las condiciones sociales adecuadas, gente decente, ordinaria, puede ser conducida a realizar cosas extraordinariamente crueles”.<sup>295</sup>

En efecto, los personajes más brutales de la película son gente de rutinas muy comunes. Alias “H” es un buen marido y padre ejemplar pero, al mismo tiempo, es capaz de causar los mayores sufrimientos a un hombre cautivo. La agente Brody encara a Rina, mujer de alias “H”, y le reprocha la incongruencia de vivir con un hombre que no es normal, a lo que ella exclama:

## Gestión de Inteligencia en las Américas

“¿Normal? Deje que le cuente algo. Perdí a mi primera familia en Bosnia. Tres hombres vienen a mi casa. Me violan frente a mi familia y después matan a todos. A mi niño pequeño lo matan el último. Esos eran mis vecinos, me conocían. Hombres muy normales”. Rina por su parte, es una mujer hermosa, de modales agraciados, y aparentemente frágil. Su pasado, no obstante, revela hechos impensables según relata alias “H”: “¿Le contó el final de la historia? ¿lo que ocurrió cuando recuperaron el poblado y capturaron a los tres hombres?. Ella mató a sus esposas e hijos frente a ellos. Y justo cuando llegaban nuestras tropas mató a esos tres hombres. La arrestaron y la pusieron a mi custodia”.

Los estándares morales actúan normalmente como auto reguladores de la conducta, sin embargo, existen mecanismos por los que se puede desvincular el comportamiento de los patrones de moralidad. Bandura lo llama “desenganche” o “abdicación” moral selectiva.<sup>296</sup> En las fases tempranas de desarrollo, la conducta es regulada por dictámenes externos y sanciones sociales. En el curso de la socialización, cada persona va adoptando estándares morales que le sirven de guía y base para la autorregulación de la conducta. El ejercicio de esta moralidad tiene un comportamiento dual: un forma inhibitoria -el poder de restringirse de comportarse inhumanamente- y una proactiva, expresada en el poder de comportarse humanamente. La gente busca “hacer lo correcto” para no caer en auto devaluaciones.

Estos estándares morales, sin embargo, no actúan de manera invariable. La activación o desactivación selectiva de este control personal, enmarcada por factores ambientales, sociales y psicológicos, permite que una misma persona se comporte de diferente manera en situaciones distintas. Las personas normalmente no se involucran en actividades consideradas “inaceptables” mientras no las hayan justificado. Este proceso de justificación moral permite que la conducta reprobable sea personal y socialmente admisible. No se trata de transformar las estructuras de personalidad o de valores, sino más bien, en redefinir la moralidad de las acciones reprobables de tal modo que puedan ser emprendidas libres de autocensura.

En el Figura 5 se muestran los posibles puntos de quiebre del autocontrol moral, que permitirían justificar la perpetración de inhumanidades.

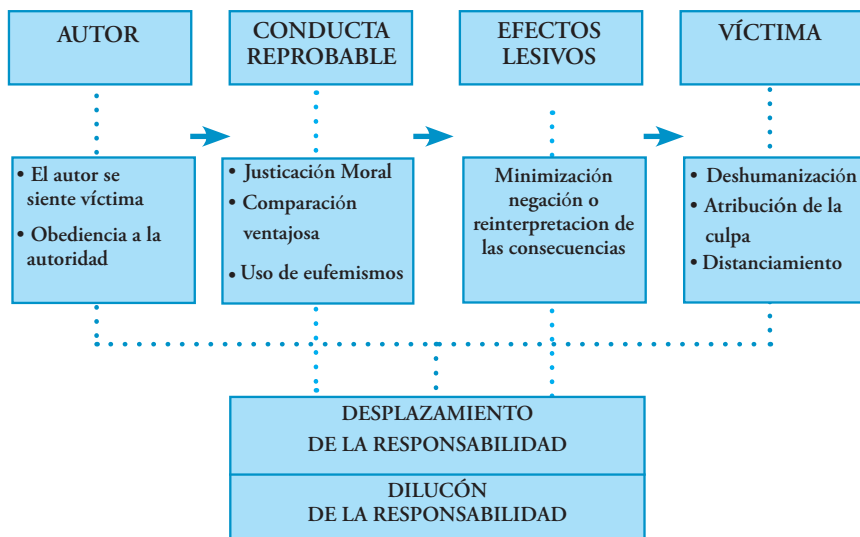


Figura 5. Principales Justificaciones para las Conductas Inhumanas. Fuente: Elaboración de los autores (2012), adaptado de Albert Bandura, “Moral Disengagement in the Perpetration of Inhumanities,” *Personality and Social Psychology Review*, 3, no. 3 (1999), p. 194.

A menudo, el ejecutor de la violencia se considera una víctima: ha sido humillado, derrotado, tratado injustamente. Esto le da derecho a atacar, ya sea en defensa propia, o como una forma de reparación. La obediencia a la autoridad y la participación en una empresa grupal permiten también que la responsabilidad se desplace y se haga difusa. La conducta reprobable se legitima apelando a la reciprocidad frente a las acciones del enemigo. Estando en juego el honor o la supervivencia del grupo, además, empieza a imperar la “moral del resultado”, es decir: el fin justifica los medios. El lenguaje ayuda a suavizar los significados de las transgresiones a través de eufemismos, tales como: “defensa”, “limpiar”, “incidente”, “daño colateral”, “retirar”, etc. Otra forma de debilitar el control moral es a través de la distorsión de las consecuencias de las propias acciones: negarlas o minimizarlas, o bien desacreditar la evidencia es útil en este sentido. Finalmente, con respecto a la víctima, se toma la mayor distancia posible, tanto física (facilitado por las armas modernas), como psicológica (al atribuirle el ser distinto, traidor, infiel, etc.). Si se le quita su humanidad, asimilándola con algún parásito, animal o enfermedad,

## Gestión de Inteligencia en las Américas

no sólo es más dable atacarla, sino que se reformula la acción como beneficiosa y necesaria.

En “*Unthinkable*” las autoridades se sienten ridiculizadas por una amenaza catastrófica que no previeron. Esto les autoriza para defenderse privando de libertad a alguien arbitrariamente. Se debe obedecer a la autoridad central: “El alto mando cree que todos deberíamos hacer lo que creamos mejor por nuestro país y su gente”. La presencia del representante del gobierno resta responsabilidad a los mandos militares. El General Paulson da órdenes al Coronel Kerkmejian y éste a sus soldados, pero el verdugo no tiene un jefe directo y la agente del FBI asiste como observadora. Se trata de una tarea colectiva que un solo hombre ejecuta pero que todos aprueban indirectamente. Es una actuación reprochable para algunos y quizás ilegal, pero si ocurre el desastre, ellos mismos se representan, desaparecerá la legalidad completamente.<sup>297</sup> La tortura, explica alias “H”, no se está aplicando a una persona en particular, sino que se está consiguiendo información del único modo posible para enfrentar la debilidad y el temor. Mediante la reformulación, la comparación, y el uso de eufemismos, se llega, finalmente, a justificar la conducta inhumana, importando sólo el resultado que desean.

### Conclusiones

Es tarea de la gestión de inteligencia aplicar la ética pública. El “deber ser” del agente de inteligencia, en un Estado de Derecho, se debe estructurar sobre fundamentos legales y éticos basados en el respeto de la dignidad de la persona. El profesionalismo de los servicios de inteligencia implica una sólida formación legal y valórica, y una permanente supervisión interna capaz, entre otras cosas, de inhibir el surgimiento de eventuales “identidades recelosas” que alienten actuaciones desmesuradas en situaciones de crisis.

La película “*Unthinkable*” o “El día del juicio final” de Gregor Jordan (2009) presenta una versión actualizada del ya clásico caso de la “bomba de relojería”, también llamado “*TickingTime-Bomb Scenario*”. En él se plantea la posibilidad -o “necesidad”- de extraer información mediante suplicios para salvar la vida de muchas personas inocentes. Un análisis serio de la película y del entorno de la inteligencia policial permite concluir que las premisas sobre las cuales se estructura el caso es excesivamente artificiosa, y una interpretación psicológica de la misma sugiere que no puede justificarse la tortura como

una herramienta para la búsqueda de información, incluso en un escenario de crisis.

Esta película y otras mencionadas en el ensayo ofrecen una reseña útil de las buenas y malas prácticas de los servicios de inteligencia, entre los que operan en un Estado de Leyes. En su totalidad, permiten generar una discusión teórica, de importantes alcances prácticos, sobre la necesidad de adecuar los métodos de inteligencia, y contrainteligencia, a los parámetros jurídicos y éticos de los derechos humanos.

### Referencias de Filmografía

CONTACTO EN FRANCIA, [DVD]. William Friedkin. Estados Unidos, D'Antoni Productions, Schine –Moore Pro.

EL DIA DEL JUICIO FINAL, [DVD]. Gregor Jordan, Estados Unidos, Lleju Productions and Films y Sidney Kimmel Entertainment International: 2009. (97 min).

EL SECRETO DE SUS OJOS, [DVD]. Juan José Campanella, Argentina, Tornasol Films, Haddock Film, 100 Bares, Telefe y otros: 2009. (129 min).

QUÉMESE DESPUÉS DE LEERSE, [DVD]. Joel y Ethan Coen. Estados Unidos, Bronx Community College, University Avenue at West 181 Street, Bronx, New York City y otros: 2008. (96 min).

LA BATALLA DE ARGEL, [DVD]. Gillo Pontecorvo. Italia y Argelia, Igor Fil y Casbah Film: 1966. (121 min).

LA CIUDAD DE LAS TORMENTAS, [DVD]. Paul Greengrass. Estados Unidos, Universal Pictures, Studio Canal y Relativity Media: 2010. (115 min).

LA VIDA DE LOS OTROS, [DVD]. Florian Henckel von Donnersmarck, Alemania, Wiedermann & Berg Filmproduktion, Bayerischer Rundfunk, Arte y Creado Film: 2006. (137 min).

LOS INFILTRADOS, [DVD]. Martin Scorsese. Estados Unidos, Warner Bros. Pictures, Plan B Entertainment, Initial Entertainment: 2006. (151 min).

## Gestión de Inteligencia en las Américas

Una versión distinta de este artículo apareció en las jornadas de derecho público 2012 en la Pontificia Universidad Católica de Valparaiso, Chile.

### Biografías de los autores

**Moira Nakousi Salas.** Médico Psiquiatra. Psiquiatra clínica y miembro del Consejo de Calificación Cinematográfica de Chile. moira.nakousi@gmail.com.

**Daniel Soto Muñoz.** Abogado, Profesor e investigador de la Academia de Ciencias Policiales de Carabineros (ACIPOL). Consultor en derechos humanos y derecho humanitario. dansotocl@yahoo.es.





## Inteligencia, Medios de Comunicación y Discurso Político

Manuel I. Balcázar Villarreal

Una fiscalización eficaz de la inteligencia en el contexto democrático depende de una relación confiable entre los responsables del desempeño de la función inteligencia estratégica y, por otro lado, la clase política en tanto representan los intereses de los ciudadanos. Para interceder en esa relación, la opción más directa y eficiente es el empleo electivo y concienzudo de los medios masivos de comunicación para abordar el tema de la importancia estratégica y los usos legítimos de inteligencia. Sin embargo, hasta la fecha se nota una falta del mismo y grandes oportunidades para desarrollar esta relación.

A partir de la primera década del siglo XXI, con entorno de seguridad complejo a nivel nacional y crisis internas en varios países del hemisferio occidental, así como el auge democrático para la elección de gobernantes, los servicios de inteligencia han cobrado mayor presencia en el discurso político y los medios de comunicación.

Sin embargo, se registra una paradoja para el concepto de inteligencia, ya que aún cuando tiene mayor presencia en medios y los jefes políticos hablan con más frecuencia del término, más confusión se genera, al no abordar el tema con el rigor apropiado o desde la visión de actores especializados, como puede ser la academia o los organismos gubernamentales responsables del tema.

Las referencias mediáticas encontradas generalmente hacen alusión a las organizaciones de inteligencia para la seguridad, difundiendo en ocasiones los “logros” (capturas) de sus servicios con el apoyo de los directores para posicionar su organización o imagen pública, siendo esto meras referencias que poco ayudan a un debate serio del tema. Ejemplos se encuentran en las recientes capturas de presuntos traficantes de drogas en Argentina, Colombia y México.<sup>298</sup>

Otro de los elementos que vincula a la inteligencia con los medios de comunicación son las filtraciones de productos o revelaciones de personal de los servicios de inteligencia, en activo o retirados, que la mayoría de las veces cometen estas infidencias por resentimiento con sus organizaciones y los métodos con que se otorgan los recursos o ascensos al interior de las mismas. Este tipo de

revelaciones suelen tener menos frecuencia pero mayor impacto para las organizaciones de inteligencia, ya que normalmente su contenido está diseñado para dañar a las organizaciones por personas que conocen el funcionamiento de la actividad y el ciclo de inteligencia.

Sin embargo, pese a ser difundidas en distintos medios de comunicación, este tipo de revelaciones encuentran poco eco en la opinión pública no especializada, que está más familiarizada con la inteligencia contra amenazas específicas, como pueden ser “peligrosos criminales”, “malvados terroristas” o “personajes desquiciados”, que se presentan en medios de comunicación como oportunamente capturados por las fuerzas de seguridad y ganan notoriedad especial.

Esto muestra una propensión mediática a tratar los temas de inteligencia exclusivamente desde una vertiente operativa, que es la que trasciende frecuentemente a los círculos políticos, que gradualmente incorporan el uso del término a sus discursos como sinónimo de investigación con resultados aptos para ser difundidos.

Así la inteligencia en su vertiente operativa ha comenzado a utilizarse con más frecuencia por los cuerpos de policía para transmitir en medios de comunicación sus logros en la captura de delincuentes. Sin embargo no se difunden planes delictivos frustrados por la acción policial, o acciones preventivas para la reducción de índices delictivos, que implicaría un manejo de la inteligencia estratégica más desarrollado, que hasta ahora se encuentra lejos de las policías.

De esta manera es frecuente encontrar en los medios de comunicación declaraciones o comunicados de prensa en los que se informa que las policías realizaron “tareas”, “trabajos” o “labores” de inteligencia para debilitar a la delincuencia, logrando normalmente la captura de armas, cartuchos, personas, vehículos y equipos de comunicación. Sin embargo poco se sabe de las tareas de inteligencia financiera para afectar las estructuras de las organizaciones delictivas, ya que ello implica mayor complejidad técnica y el manejo de otras vertientes de inteligencia.

Pese a las confusiones conceptuales que genera el tratamiento policial de la inteligencia en medios de comunicación, se aprecia una muy buena relación entre medios y jefes de policía, que construyen carreras políticas, logran mayor

## Gestión de Inteligencia en las Américas

presupuesto o se posicionan frente a otras agencias gracias a la difusión operativa del concepto de inteligencia, que les ayuda a construir una percepción pública de profesionalismo y generar expectativas por arriba de las capacidades existentes. Al respecto tanto México, Colombia y Perú han tenido en las dos últimas décadas casos con estas características.

Esta circunstancia nos remite al tratamiento de la inteligencia a mediados del siglo XX en varios países de Centro y Sudamérica, que empleaban las capacidades de investigación de sus policías para fines políticos asociados a la estabilidad y control, que limitó las capacidades y desarrollo de los servicios de inteligencia, al desarrollar esquemas de profesionalización asociados a la vertiente operativa y no estratégica, privilegiando aptitudes físicas de sus elementos sobre las analíticas.

La imposición del enfoque de inteligencia operativo sobre el estratégico ha derivado en prácticas empíricas mayoritariamente operativas dentro de las organizaciones de inteligencia, que actualmente persiste en algunos países, y “seduce” a los funcionarios que encabezan servicios de inteligencia por primera vez cuyo contacto previo con la inteligencia es normalmente mediático.

Otra de las vertientes que da cuenta de la relación entre medios e inteligencia es el espionaje político y la revelación de conversaciones o videos en situaciones comprometedoras de actores políticos, que no tiene ningún objetivo de inteligencia, sino busca generar confrontaciones políticas o arruinar carreras, mediante los escándalos que detonan las filtraciones de conversaciones privadas. Al respecto los espías suelen responder con cuestionamientos sobre la legalidad o ética para la intervención y registro de actos privados, tratando de evitar explicar el contenido de sus actos.

Debe mencionarse que esta práctica de espionaje suele tener mayor recepción en los medios de comunicación y sociedad en general, generando una percepción distorsionada del concepto de inteligencia, que se aborda en genérico, sin especificar características de inteligencia gubernamental y, generando como resultado una cultura incorrecta en la materia.

Con estas percepciones distorsionadas que son generadas en el seno del empirismo de organizaciones que realizan actividades de inteligencia, y reproducidas por los medios de comunicación, la clase política gradualmente

y de manera tímida han comenzado a incorporar el concepto de inteligencia a sus discursos, haciendo de él una respuesta política o una oferta institucional con la que se comunican con la sociedad y transmiten tranquilidad al prometer que se realizará inteligencia para enfrentar un riesgo o amenaza en específico.

Todas estas circunstancias representan un reto para la gestión de inteligencia en el Siglo XXI, frente a un contexto mediático de desinformación sobre la naturaleza de la inteligencia, que refleja en el discurso político y algunas propuestas de políticas públicas o acciones de gobierno una conceptualización de inteligencia que apoya al mantenimiento del desarrollo inercial de las burocracias de inteligencia, limitando la capacidad de analizar, debatir, mejorar y profesionalizar los servicios de inteligencia.

La alternativa para revertir este proceso disfuncional en el triángulo inteligencia, medios de comunicación y discurso político puede construirse desde los medios de comunicación, estableciendo vínculos con investigadores y académicos, además de revisar literatura especializada sobre inteligencia para contextualizar los reportes gubernamentales, además de cuestionar y evaluar el discurso y propuestas políticas de los tomadores de decisiones, que ante la confusión parecen haber iniciado el uso abusivo del concepto de inteligencia.

**Manuel I. Balcázar Villarreal** es Maestro en Administración Pública por el Instituto Nacional de Administración Pública (INAP-México); graduado del Centro de Estudios Hemisféricos de Defensa (CHDS), de la Universidad de la Defensa Nacional (NDU), Washington, DC. Cursó el Seminario de Prevención del Delito del Centro de Estudios sobre Seguridad Ciudadana de la Universidad de Chile, obteniendo la distinción máxima. En 2008 fue becario del Departamento de Estado Norteamericano en el curso de Asuntos del Crimen Organizado Internacional. Fue Director General Adjunto de Seguridad Nacional en la Presidencia de la República (México). Actualmente es docente del Diplomado de Seguridad Nacional de la Universidad Iberoamericana y consultor independiente. Es autor del libro *La influencia de las maras en México: un problema de inteligencia gubernamental* (INAP, 2007); así como del volumen *Inteligencia Estratégica en el Contexto Mexicano*, publicado en 2012 por el Tecnológico de Monterrey, entre otros.  
Correo: [ibavil@hotmail.com](mailto:ibavil@hotmail.com).

## Sección II

# Gestión de Inteligencia en la Rama Ejecutiva de los Gobiernos



## Gestión de Inteligencia en las Américas

### Procesos de Toma de Decisión Presidencial en Inteligencia—una Cuestión Pendiente

Guillermo Holzmann

#### Resumen

El presente artículo plantea un análisis descriptivo, desde una óptica politológica, orientado a identificar el rol y características de los productos de Inteligencia en los desafíos derivados de los procesos de toma de decisión presidencial en democracias emergentes de América Latina para enfrentar los escenarios de desarrollo político en su amplia cobertura. Para ello, se analiza el contexto en el cual se desenvuelve el proceso decisional democrático. Este estudio constituye la primera parte de un esfuerzo más amplio que permita establecer las características objetivas tendientes a superar las insuficiencias y vacíos institucionales en el uso de los productos asociados a un sistema nacional de inteligencia.

#### Introducción

El proceso de globalización ha demostrado que aquellos países que no se adaptan a las condiciones y exigencias provenientes del sistema internacional, especialmente en lo económico y en lo político, reducen drásticamente sus posibilidades de alcanzar niveles importantes de crecimiento con el fin de generar la plataforma necesaria para consolidar el desarrollo de sus sociedades. En este sentido, surge como un imperativo la necesidad de replantear y ampliar la identificación de intereses nacionales, más allá de los clásicos expresados en documentos oficiales.<sup>299</sup> Ello implica una metodología que permita, de manera explícita y bajo criterios deductivos e inductivos, analizar y establecer los desafíos tradicionales y nuevos, bajo parámetros que superen, por ejemplo y como mínimo, los períodos presidenciales, y con una fórmula de legitimidad compartida por la elite y comprendidos y asumidos por la sociedad.

Las visiones sobre la dinámica mundial en sus distintas dimensiones poseen una diferencia notable entre aquellos países desarrollados, que lideran el proceso de cambios estructurales asociados a la globalización, en comparación con los ubicados en América Latina, para quienes este proceso los obliga a enfrentar aspectos no resueltos del siglo XX (pobreza, desigualdad, confrontación



ideológica entre capitalismo y comunismo y la permanente búsqueda de un desarrollo social, entre otros), sino también y en forma simultánea asumir el desafío de insertarse plenamente en el entorno mundial. Estas cuestiones exigen, entre otros aspectos, una incorporación de factores y variables para el diseño de políticas públicas asociadas a nuevos roles del Estado y gobiernos más eficientes y oportunos. En suma, se trata de un escenario donde las condiciones mínimas de gobernanza se implementan conforme las capacidades de cada gobierno, privilegiando aspectos de estabilidad y gobernabilidad. La exigencia de adaptación tiene un impacto directo en el diseño de los procesos decisionales a nivel ejecutivo, donde es necesario dar cuenta de las deudas sociales y políticas del pasado y simultáneamente se precisa establecer caminos futuros bajo condiciones de oportunidad y anticipación decisional.

En efecto, uno de los elementos de mayor significación en la conducción política del Estado en el siglo XXI, está asociada a la capacidad del manejo y procesamiento de información para establecer escenarios futuros. De interés es la correspondiente identificación de factores y variables, en los cuales se reconozcan probables amenazas, riesgos y oportunidades en horizontes de mediano y largo plazo. De esa manera, se puede aportar a un proceso de toma de decisión gubernamental, en un esquema democrático de características complejas, y sometido a la influencia de múltiples intereses correspondientes a distintos actores estatales, no estatales y privados, tanto nacionales como extranjeros.

Los países de América Latina presentan notables diferencias en sus grados de desarrollo y niveles de crecimiento. Si bien pueden ser catalogados como países emergentes, ello difiere de la percepción existente frente a la situación de Brasil, India y otras potencias medianas. La calidad de país emergente,<sup>300</sup> supone la generación de condiciones y la consolidación de características políticas, económicas y sociales determinantes para el logro de una adecuada inserción internacional para la satisfacción de los intereses nacionales. Lo razonable sería plantear que los países de América Latina poseen similares desafíos que las potencias medianas pero sin tener una plataforma socio-económica y política similar. Es justamente en la convergencia de objetivos estratégicos de países que comparten intereses similares donde se requiere una mayor preocupación en la producción de inteligencia estratégica.

## Gestión de Inteligencia en las Américas

En este contexto, la existencia de un sistema de inteligencia en el nivel estatal, cuyos productos sean un insumo considerado seriamente en el proceso decisional y que integre los distintos organismos de inteligencia que cada país posee y establezca una diferenciación nítida entre los distintos niveles en los cuales la inteligencia se puede desarrollar, constituye una exigencia de la globalización. Su límite está asociado a los requerimientos del régimen democrático y, en especial, a la presencia de adecuados controles y procesos de regulación política.

Así, cada Estado ha enfrentado, en distinta forma, el desafío de modernizar, transformar y/o crear sistemas de inteligencia orientados a satisfacer las necesidades de los procesos decisionales, con un evidente cambio respecto a su función en la guerra fría que se centraba, básicamente, en la identificación y neutralización de amenazas ya sea de origen interno o externo y que respondían a la definición de un enemigo concreto y, por tanto, privilegiaba una respuesta de carácter militar. No obstante ello, tal proceso enfrenta en la actualidad obstáculos políticos, económicos y, en especial, conceptuales para establecer el sistema de inteligencia más adecuado a cada país. Ello es particularmente válido para los países de América Latina clasificados como emergentes. Los niveles de decisión presidencial requieren de organismos de inteligencia basados en una construcción sistémica acorde sus intereses de proyección global, regional y nacional, donde las capacidades militares y policiales son necesarias pero no suficientes para abordar los nuevos escenarios.

### Relación inteligencia y política

Los Estados en América Latina han tenido una evolución diversa sobre los sistemas de inteligencia y sus organismos, conforme sean las perspectivas desde la cual se construyan sus aproximaciones. Están aquellas provenientes de la academia y centros de estudios con una evidente influencia de Sherman Kent; otros están basadas en el aporte de la inteligencia militar. Otros tipos dan cuenta de una evolución con distintas características, hasta las visiones más políticas e ideológicas respecto a su rol y funciones en los regímenes dictatoriales o autoritarios y su vinculación con la violación de derechos humanos.<sup>301</sup> A ellas se suma una percepción social basada en particulares cosmovisiones mostrando una débil cultura de inteligencia en los distintos niveles de la sociedad.<sup>302</sup>

Desde la década de los 80's, cada país ha desarrollado y modificado sus estructuras de inteligencia bajo condiciones democráticas expresadas en legislación, controles y niveles de conducción civil que incorporan características orientadas a establecer la coordinación de los organismos militares y policiales y, en algunos casos, generar organismos superiores de soporte y apoyo a la conducción política.

Más allá de los recursos humanos e institucionales diseñados y establecidos por los países para configurar su sistema de inteligencia, un problema central es la construcción de una relación efectiva entre quienes producen inteligencia (producción de información útil), los niveles de toma de decisión en los cuales se inserta y, finalmente, la consideración que sobre los insumos anteriores tenga el decisor para definir la acción a implementar. Para los países de América Latina el imponer la definición de una vinculación institucional, funcional y eficiente constituye un imperativo para obtener condiciones de ventaja en la exploración en impactos, oportunidades y neutralización de riesgos y amenazas que afectan el nivel superior de la conducción gubernamental.

Sin embargo, la construcción de una relación efectiva y productiva entre los usuarios de inteligencia y los productores exige que la información y el análisis de inteligencia sea oportuno, profesional y confiable, considerando que el decisor también accede a otros insumos provenientes de asesores, centros de estudios o *Think Tank* cuya finalidad es influir en la agenda gubernamental, presionar por determinadas decisiones o simplemente plantear argumentos para defender intereses.

De esta forma, el producto de inteligencia precisa conocer la orientación del decisor con la finalidad de entregar un insumo o producto adecuado a sus necesidades del momento, donde la anticipación respecto a los objetivos o ejes prioritarios del decisor es un aspecto central. Del mismo modo, la inserción de la inteligencia en el proceso decisional debe tener un tratamiento diferenciado respecto a otros insumos, debido a su naturaleza no-partidista y centrada en los objetivos del Estado expresados en el Gobierno.

Por ello, la necesidad de una institucionalidad sólida orientada a la optimización del proceso decisional es fundamental. El diseño de los procesos decisionales y la presencia de una institucionalidad adecuada, permanente en

## Gestión de Inteligencia en las Américas

el tiempo y reconocida en la gestión estatal constituyen un déficit en varios sistemas de América Latina. Un sistema de inteligencia adecuado cuenta con una diferenciación clara entre los niveles junto con incorporar controles y protocolos en el manejo de información tendiente a evitar su filtración o mal uso. A ello es preciso incorporar prácticas de coordinación efectivas para labores interagenciales al interior del Gobierno.

Un sistema de inteligencia en pleno funcionamiento, con sus respectivos niveles, controles democráticos y recursos adecuados significa una institucionalidad definida desde el nivel superior del Estado, evitando la hipertrofia de organismos básicos, como es el caso de la inteligencia militar o policial. Al no existir una estructura civil de mayor nivel y profesionalismo, terminan desarrollando una inteligencia táctica, operacional y estratégica y además nacional, con lo cual se desvirtúan sus roles y funciones y se deslegitima el sentido de un sistema nacional de inteligencia.

En aquellos países que mantienen un diseño institucional tradicional en términos de una arquitectura organizacional del Estado más rígida y con menor capacidad de adaptabilidad y coordinación interagencial en sus procesos, como sucede con varias democracias en América Latina,<sup>303</sup> la utilidad de la inteligencia en el más alto nivel político suele transitar en, al menos, los siguientes usos:

- a. La inteligencia es utilizada con fines específicos para mantenerse en el poder y neutralizar posibles adversarios o justificar la propia acción política en una mirada coyuntural o de corto plazo. En este caso la inteligencia se personaliza y politiza.
- b. La inteligencia se concibe en términos reduccionistas y focalizada al control y neutralización de conflictos sociales o riesgos -si es que no amenazas- a la permanencia del gobierno de turno. En este caso, se trataría del uso de la inteligencia para el control social.
- c. La inteligencia política está al servicio del gobernante y su gobierno. Los demás organismos de inteligencia cumplen su función con distintos grados de autonomía según criterios institucionales que no necesariamente coinciden plenamente con los gubernamentales.

Adicionalmente, la tendencia a designar “personas de confianza política” antes que asegurar calidad, eficiencia y oportunidad en los equipos de análisis

impide la capitalización de experiencias, la incorporación de buenas prácticas y un sentido ético en el desarrollo de las actividades de la inteligencia para el nivel político.

Al prevalecer el criterio de confianza política en los niveles de análisis, la tendencia natural será la producción de inteligencia de corto plazo y centrada en aspectos específicos de interés gubernamental, dejando de lado la construcción de escenarios y la identificación de los factores de cambio que, en términos domésticos o internacionales, pueden afectar directamente los intereses del país y su seguridad. En este sentido se produce una paradoja: por una parte se produce inteligencia de corto plazo que ayuda a decisiones reactivas frente a los acontecimientos de corto plazo y se evita la producción de inteligencia de largo plazo y estimativa que podría dar mejores factores de éxito al gobierno de turno. Ello termina produciendo una desprofesionalización de la inteligencia estratégica de Estado y una desnaturalización de las funciones y roles de los organismos de inteligencia en los distintos niveles del sistema. El resultado inevitable es la inexistencia de una continuidad en el proceso decisonal de nivel estratégico cuyos costos aumentan en forma correlativa con los cambios de dirección en la conducción del sistema de inteligencia.

Bajo estos parámetros, por ejemplo, la interrelación con otros organismos de inteligencia de países amigos, es afectada de modo negativo al no existir horizontes de mediano y largo plazo en los análisis, con lo cual no se logra un intercambio profesional de información y de análisis en temas comunes para los países, privilegiándose un trabajo más informal con cada organismo por separado y cuyo resultado es un lento proceso de deslegitimación del sistema de inteligencia, por bajos estándares de profesionalización. Las implicancias son variadas y no siempre de interés del decisor, no obstante la exigencia internacional de mantener un sistema validado como interlocutor en ámbitos de interés internacional.<sup>304</sup>

Los productores de inteligencia estratégica (entendida como Nacional o Presidencial) muchas veces no juegan un rol fundamental en los procesos decisonales de los gobernantes en temas de estrategia nacional ni en temas de seguridad nacional. Más aún, cabe cuestionarse si los tomadores de decisión tienen la posibilidad o capacidad de usar los productos de inteligencia. Las preguntas derivadas de este planteamiento son diversas y de amplio espectro, pues suponen una auditoria al proceso de toma de decisiones estratégicas.

## Gestión de Inteligencia en las Américas

Sobre la vinculación entre inteligencia y política<sup>305</sup> se precisa mayores estudios para abordar ya no sólo las dificultades históricas heredadas de distintos procesos políticos, sino para establecer los desafíos que existen a futuro. En cada país de América Latina existen especialistas civiles y militares que han aportado a la comprensión de la inteligencia y sus implicancias en política. No obstante ello, consideramos todavía escasa la bibliografía<sup>306</sup> existente. La problemática dice relación con las características del sistema de inteligencia, su capacidad real de coordinación y dirección, como también los estándares profesionales y éticos asociados a su capital humano. De allí se derivan los desafíos en cuanto a reclutamiento, metodologías de análisis y capacidad de generar escenarios de anticipación. Desde la perspectiva política, tenemos la necesidad de avanzar en una mayor y mejor cultura de inteligencia, el diseño de procesos decisionales asociados a una burocracia especializada en el nivel presidencial que se mantenga en el tiempo y pueda ejercer la interlocución política con los organismos del sistema, especialmente con su ente coordinador.

Un estudio de Ohad Leslau<sup>307</sup> -y que referiremos a continuación- revisa algunas aproximaciones interesantes de considerar al momento de establecer los lineamientos teóricos acerca del rol de la inteligencia durante los procesos de toma de decisión. Dichos estudios pueden ser divididos en tres tipos, de acuerdo al nivel de análisis involucrado: individual, organizacional-burocrático, y estatal.

En el nivel individual, se examina cómo el carácter de específicos decisores y productores de inteligencia influye en forma determinante en el producto de inteligencia. Ello supone focalizarse en las características psicológicas de cada uno de los actores -decisor o productor- asumiendo distintos enfoques con la finalidad de estudiar la relación que se establece entre el decisor y el producto de inteligencia recibido. Desde una perspectiva distinta se abordan las características psicológicas del proveedor de inteligencia. Con ello se busca establecer la manera en que la metodología utilizada en los análisis y el perfil psicológico de los productores de inteligencia puede ser determinante en la forma en que su labor es percibida y recibida por los decisores.

Este tipo de estudios, conforme señala Leslau, suelen estar influidos por estudios normativos, los cuales distinguen entre aquellos analistas que desarrollan la inteligencia en forma profesional y aquellos que proveen inteligencia política. Los primeros son cautelosos y cuidadosos para solo

ofrecer su opinión técnica y profesional, sin abordar los aspectos políticos, mientras que los segundos poseen mayor involucramiento en los factores que definen el escenario político. La necesidad de un espacio de convergencia en el entorno inmediato del gobernante es crucial para establecer una relación fluida y confiable.

Las investigaciones referidas al nivel organizacional-burocrático están basadas en los trabajos teóricos de Graham Allison.<sup>308</sup> En ellos se explica que los organismos de inteligencia juegan un rol equivalente al de otras agencias e instituciones gubernamentales y estatales. De esta forma, el grado de influencia del producto de inteligencia está determinado por el estatus y prestigio de la agencia de inteligencia al interior de la burocracia gubernamental. De esta forma, si un organismo de inteligencia se encuentra más cercano a los círculos de poder y decisión, como es el caso de Cancillería o Ministros de Interior o Presidencia, su grado de influencia en el proceso decisional se incrementa.<sup>309</sup>

Las investigaciones sobre el rol de la inteligencia a nivel presidencial, dan cuenta de cómo ciertas características de un Estado definen el grado de influencia por el cual el producto de inteligencia contribuye al proceso de toma de decisiones. Las tres variables principales en que se concentran estos estudios son: el tipo de régimen, la gravedad de la amenaza que se enfrenta, y la “cultura de inteligencia”. Se concluye que el producto de inteligencia tendrá mayor legitimidad, por sus controles e inserción en el sistema decisional de política exterior cuando se trata de regímenes democráticos antes que totalitarios o autoritarios, en virtud de que el objetivo de regímenes de esta naturaleza responden a la proyección del líder y su pensamiento, confundiendo los intereses nacionales con los objetivos políticos del dictador que empiezan por su mantención en el poder a todo evento. El caso de Corea del norte es probablemente el ejemplo más real en este sentido. Otro punto a considerar en el ámbito de la influencia de los organismos de inteligencia se relaciona con la identificación de amenazas a valores esenciales del Estado, en estos casos la inteligencia se transforma en un factor dominante en el proceso de toma de decisiones.

En esta perspectiva, Leslau plantea algunas debilidades de los estudios reseñados, en términos de sus reales capacidades para medir y explicar la influencia de la inteligencia en cuestiones de decisión nacional. Por una parte, señala la falta de una explicación más amplia, en términos de variables, respecto a cuándo y cómo el producto de inteligencia influye en los procesos

## Gestión de Inteligencia en las Américas

decisionales de nivel presidencial. Ello considerando las distintas dimensiones y niveles de análisis necesarios para obtener productos de inteligencia acorde a las expectativas y necesidades de los decisores. La segunda debilidad se refiere a la metodología de estudio en este campo. Al efecto, las investigaciones se centran en casos específicos o en un solo decisor desde donde se plantean generalizaciones no confiables en sus conclusiones. A nuestro entender, es necesario considerar el proceso de toma de decisión en un sentido sistémico, con sus factores y externalidades, donde los productos de inteligencia alimentan distintos niveles, empezando por el presidencial. Ello define productos diferenciados y especializados.

En América Latina la carencia de institucionalidad presidencial que incluya la inteligencia, bajo parámetros adecuados de gobernanza, constituye un problema en términos de carecer de insumos relevantes para la gestión estratégica superior del Estado y el Gobierno. Se trata de una cuestión estructural respecto a la instalación de una alta burocracia a nivel presidencial que responda a un criterio de permanencia y supere cada período gubernamental y una cuestión funcional asociada a la necesidad de procesar análisis y genera opciones con sentido estratégico más allá de las necesidades gubernamentales de corto plazo.

En suma, la gestión de inteligencia en las ramas ejecutivas de los gobiernos de América Latina en general, es aun débil en términos organizacionales, estructurales, de procesos y profesionalismo.

Sin embargo, en la medida que aumenta el grado de inserción internacional de un país, definitivamente la exigencia de coordinación interagencial y la existencia de sistemas de inteligencia y organismos especializados -más allá de lo militar y lo policial- constituyen un requisito para los decisores políticos. Igualmente, existe la necesidad de replantear la legislación sobre inteligencia para obtener reglamentos y productos de inteligencia destinados a consolidar y cooperar a la gestión integral del Estado.

### Reflexión final y presentación de artículos

En este capítulo se abordan aspectos necesarios de estudiar y debatir en términos de diagnóstico de los escenarios de la inteligencia y sus problemáticas asociadas.



Mariano Bartolomé, por ejemplo, en su ensayo “La Inteligencia Estratégica y sus requisitos para la seguridad de América del Sur”, desarrolla un amplio diagnóstico respecto a los desafíos que enfrenta la inteligencia estratégica en Sudamérica. Por una parte se reconoce la persistencia de las visiones tradicionales de conflicto derivadas del realismo en las relaciones internacionales, cuya principal responsabilidad recae en las capacidades militares en el área de la defensa y aquellas que estando más asociadas al crimen organizado y bajo un prisma asimétrico complican en distintas dimensiones del desarrollo a los países, especialmente en lo que se refiere al impacto del terrorismo, el narcotráfico y el tráfico de personas. Una perspectiva que enfatiza no sólo la necesidad de contar con un sistema de inteligencia maduro sino con una gestión de sus productos orientados al decisor gubernamental.

Por su parte, Álvaro Venegas en su artículo, “Gestión de Inteligencia Económica Gubernamental—una propuesta para examinar en el área Andina”, desde la particularidad de la realidad de Colombia y la evolución de su situación de seguridad y la necesidad de contar con un sistema de inteligencia de mayor cobertura, plantea una propuesta orientada al diseño de un sistema interconectado, en términos horizontales y verticales, con la finalidad de generar un Sistema de Inteligencia Económica Gubernamental (IEcG), con lo cual integra a distintos subsistemas que interconectados optimizan la capacidad de procesamiento de información, la posibilidad de anticipación y la generación de productos de inteligencia y contrainteligencia. Es una propuesta que merece una detenida lectura y su respectivo debate y reflexión, tanto por su extensión como por las condiciones políticas y sociales exigibles para su implementación.

Carolina Sancho emprende un desafío significativo al estudiar y analizar las posibilidades de cooperación en el marco de UNASUR. Sistematiza la literatura al respecto y propone criterios para una configuración que en parte emula el proceso europeo para generar una orgánica al interior de UNASUR. No obstante su presentación, recoge adecuadamente los problemas que plantea la cooperación entre servicios de inteligencia, agencias o sistemas cuando no hay una cultura de inteligencia o no existen parámetros democráticos capaces de generar confianzas al interior del Estado y no existen costumbres y tradiciones de compartir información o análisis. El planteamiento teórico desarrollado plantea una exigencia de profesionalismo en la conformación de los organismos de inteligencia y una necesidad política y conceptual de

## Gestión de Inteligencia en las Américas

crear visiones convergentes respecto a los tipos de desarrollo de los sistemas de inteligencia que sean consistentes con la evolución de los países desarrollados. Entre otras cosas implica profundizar en la inteligencia orientada a las amenazas con aquella destinada a identificar oportunidades y riesgos.

Finalmente, Dan Elkins en “Gestión de Recursos para la Inteligencia” aborda un aspecto relevante de la gestión de inteligencia en una dimensión no siempre considerada. Elkins recomienda un diálogo sustantivo de gerentes de inteligencia con los parlamentos en términos presupuestarios y de programas sobre los recursos y el necesario equilibrio entre personal, presupuestos y misiones de los organismos de inteligencia, lo cual importa el manejo de herramientas, lenguaje y prácticas que posibiliten un trabajo eficiente, transparente y con capacidad de dialogar con los asignadores de recursos en el Estado y convencer además a quienes deciden sobre ello. Una propuesta técnica avalada por la experiencia personal del autor y que para el caso de América Latina constituye un aporte hacia un necesario profesionalismo de la actividad.

En síntesis, y aun cuando es evidente, no es suficiente contar con organismos de inteligencia para asegurar productos de utilidad en los niveles decisionales del Ejecutivo en la realidad de América Latina. Del mismo modo, no basta con la existencia de un Sistema para concluir que se produce información útil para el nivel presidencial. Todo organismo de inteligencia por definición produce o debiera producir información útil. Sin embargo una pregunta relevante es el destinatario de dicha información. Los organismos de inteligencia resultan poco útiles si no existe una claridad de objetivos que oriente el trabajo de análisis, los productos, destinatarios y las áreas de prioridad gubernamentales en términos de distintos horizontes de tiempo. A ello se suma, la necesidad de controles adecuados, efectivos y razonables desde el legislativo, el poder judicial y la auditoría de procesos.

En vista del actual nivel de la inteligencia en América Latina, y conforme los trabajos presentados en este capítulo algunas deficiencias importantes de considerar. Por una parte, la necesidad de fortalecer la cultura de inteligencia entre la elite política de cada país y, en especial, en los gobiernos, para obtener un mejor debate y propuestas realistas y efectivas a las problemáticas del país y no tanto a las preocupaciones cortoplacistas de los gobiernos de turno. Por otra, la existencia de un núcleo de asesoría presidencial con una burocracia permanente y donde los cambios sean de sus directivos en cada gobierno, resulta ser un

espacio ideal para la incorporación de la producción de inteligencia en el proceso decisional presidencial, independiente de aquella información útil que se haga llegar directamente al Presidente.<sup>310</sup> Es decir, una burocracia profesional tanto en la asesoría como en los organismos estratégicos de la inteligencia. Allí, las propuestas de Bartolomé, Venegas y Elkins tienen la posibilidad cierta de estudios, evaluación y propuestas de alternativas decisionales en escenarios de mediano y largo plazo, y bajo criterios de eficiencia con adecuados controles políticos, económicos, normativos y judiciales.

Finalmente, en este capítulo se abre un espacio de crecimiento en las reflexiones y propuestas sobre los temas de inteligencia en una de las áreas donde se requiere mayores aportes para nivelar la calidad de los productos que entregan los sistemas actualmente existentes y mostrar líneas de desarrollo futuro para su perfeccionamiento.

El autor **Prof. Guillermo Holzmann** es Magíster en Ciencia Política. Doctorando en Estudios Americanos, Mención Relaciones Internacionales. Académico de la Universidad de Valparaíso de Chile y la Universidad Adolfo Ibañez de Chile. Es Director del Nodo Chile de Escenarios y Estrategias (EYE), Miembro Fundador de Centro Latinoamericano de Globalización y Prospectiva, Miembro de la Red Latinoamericana de Prospectiva. Ex Subdirector del Instituto de Asuntos Públicos, Creador y Coordinador del Diploma “Metodología de Análisis de Inteligencia” en la Universidad de Chile. Asesor del Banco Internacional de Desarrollo en el Programa de Formación de Analistas de Inteligencia para Aduanas. Comentarista y analista político en diversos medios de comunicación nacional e internacional. Socio-Director de ANALYTYKA Consultores. Contacto: guillermo.holzmann@gmail.com; guillermo.holzmann@uv.cl.

### Relación entre Consumidores y Productores de Inteligencia en el Nivel Ejecutivo: Un Desafío Permanente

Manuel I. Balcázar Villareal

Quizá uno de los mayores retos para cualquier servicio de inteligencia sea la relación entre productores y consumidores, tanto por su complejidad como diferencia de ambientes en los que operan unos y otros. Las circunstancias más frecuentes en las que se enfrentan tanto consumidores como productores de inteligencia pueden hacer de su relación un gran espacio de entendimiento, o un conflictivo e ineficiente proceso en el que ambas partes se culpan entre sí, sin que la inteligencia desarrolle su función principal para el proceso de toma de decisiones.

#### Organizaciones y políticos

Pese a una mutua pertenencia al sector gubernamental, tanto productores como consumidores de inteligencia provienen de ambientes diferentes. Mientras la mayoría de los productores desarrollan sus carreras en organizaciones de inteligencia, en las que el secreto y la reserva son parte de los principios doctrinarios, los políticos se forman en un ambiente público y abierto, en el que el diálogo y acercamiento con la sociedad son una constante.

Esta situación de origen marca un fuerte diferencia entre los dos ambientes, que se acompaña de mitos asociados a la inteligencia, en los que se suelen atribuir capacidades extraordinarias a los servicios de inteligencia, y afectan el funcionamiento de la relación entre productores y consumidores. Adicionalmente debe considerarse que los servicios de inteligencia tienen una fuerte cultura organizacional que les da sentido en el largo plazo, sin embargo las desvincula de la coyuntura política y emergencias nacionales que el tomador de decisiones o consumidor tiene que resolver, y para lo cual espera apoyarse en los productores de inteligencia. Por su parte los políticos normalmente provienen de distintas ideologías partidistas o movimientos sociales, que si bien se articulan en torno al Estado – Nacional, al momento de su elección están influenciados por una gran diversidad de necesidades y demandas urgentes que resolver.

En algunas ocasiones por la formación o trayectoria de los tomadores de decisiones su relación con la inteligencia nacional es escasa o nula, por lo

cual van desarrollando su propio conocimiento junto con las tareas de gobierno, lo cual puede representar también un obstáculo para los servicios de inteligencia.

### Percepción del tiempo

Adicionalmente el uso del tiempo en las organizaciones de inteligencia y en los políticos tiene una racionalidad totalmente distinta, mientras a nivel organizacional hay certeza de permanencia y una trayectoria histórica, el líder político cuenta con períodos de 4 o 6 años de gobierno, que resultan reducidos para la atención de problemas nacionales.

Esta situación da a los productores y sus organizaciones una sensación de trascendencia y tal vez cierta autonomía frente a la problemas coyunturales, que no necesariamente tienen que resolver, ya que pueden tomar matices políticos, sociales o mediáticos, que habitualmente están desligados de la producción de inteligencia. En contraparte los líderes políticos tienen una mayor percepción de urgencia, que se incrementa con crisis o emergencias nacionales a las cuales están obligados con precisión y en poco tiempo.

Bajo este contexto es normal que los consumidores soliciten a los productores insumos para la atención de problemas específicos, lo cual hace que el trabajo de los productores se enfoque en el corto y, eventualmente, mediano plazo, sin que se desarrollen las plenas capacidades de inteligencia estratégica en el contexto nacional.

También debe de considerarse que los líderes políticos tienen un sentido que se orienta principalmente hacia la resolución de compromisos urgentes para cumplir con saturadas agendas, en las que las organizaciones de inteligencia y sus productos forman parte de un amplio mosaico de información, donde la inteligencia solo resalta en el caso de emergencias, normalmente de seguridad, diplomáticas o humanitarias.

Esto hace que el desarrollo de la inteligencia nacional normalmente oscile entre la vertiente táctica y la operativa, que es la que los productores generan de acuerdo a las necesidades de los consumidores, logrando con ello empatía por parte de estos últimos, al sentirse atendidos y escuchados, con un amplio menoscabo para el desarrollo de capacidades estratégicas, que tienen poco espacio en las agendas por no ser percibidas con rentabilidad electoral, ya que

## Gestión de Inteligencia en las Américas

los resultados de decisiones estratégicas de inteligencia difícilmente los podrá capitalizar el mismo consumidor que las asume.

### Percepciones a resolver

Quizá el principal dilema en la relación entre productores y consumidores está en la percepción y expectativas que tienen unos de otros y la manera en que se conocen y acercan estos dos componentes de la inteligencia, y que frecuentemente tienen más desencuentros que encuentros.

Ocasionalmente los productores pueden ser en extremo complacientes con los consumidores, ya que de ellos depende el presupuesto y desarrollo de las organizaciones de inteligencia, cayendo en la respuesta positiva reiterada a todas las peticiones del consumidor, sin valorar su viabilidad, impacto y utilidad para el tomador de decisiones, lo cual es sumamente perjudicial para el desarrollo de capacidades de inteligencia y profesionalización, ya que hace de las organizaciones dedicadas a la producción de inteligencia “cotos” o “feudos” de poder que se mantienen por la complacencia al consumidor, y no por la relevancia de los productos.

Otro punto central es la comunicación y la confianza que existe entre el consumidor y los productores, ya que mientras más fuerte sea el vínculo, más amplias son las posibilidades de generar productos que sean valorados, apreciados y útiles. En estos últimos elementos la entrega y presentación de los productos de inteligencia tienen un rol central, ya que de ello depende el interés y atención que pueda prestar un alto decisor en el nivel ejecutivo.

También la conceptualización propia de inteligencia en los consumidores puede ser un gran apoyo u obstáculo, pues ello define la interacción con otros actores más allá del ámbito presidencial (ejecutivo), que en el Poder Legislativo tiene un referente natural de pesos y contrapesos que puede ser de gran apoyo en la edificación y/o actualización de una política de inteligencia nacional, sin embargo consideraciones de orden político pueden empañar esta relación con una política de información restringida que en el largo plazo solamente reduce las capacidades nacionales en la material.

La incertidumbre, tanto de productores como de consumidores suele ser otro de los elementos polémicos en la relación. Para los productores en ocasiones no tienen la debida retroalimentación de los consumidores y desconocen la

utilidad de sus productos en la toma de decisiones, por ello, la comunicación y confianza con los consumidores es central. Por su parte, para los consumidores la duda se encuentra en el detalle de información que deben o pueden conocer sobre un tema en particular de acuerdo a sus responsabilidades, lo cual se vuelve más crítico si se maneja en la vertiente operativa de inteligencia.

### Resolución de un dilema

Finalmente se considera que existe la posibilidad de modernizar los conceptos y doctrina que se aplican en las organizaciones de inteligencia, así como dar un enfoque más transversal a las mismas, es decir, que sean impulsadas hacia los gobiernos estatales y oficinas públicas más allá del sector seguridad y defensa. Esto permitirá avanzar hacia una “segunda generación” que trascienda el paradigma de inteligencia tradicional de mediados del siglo XX, basado en un enfoque central. Puede ser que un enfoque más transversal apoye en el fortalecimiento de la cultura de inteligencia y sea la base para un acercamiento entre productores y consumidores, ya que así sería realizada una perspectiva estratégica de inteligencia, la cual tiende a asemejarse a la visión amplia del mundo deseado de los políticos y al que preferentemente deben acercarse los servicios de inteligencia, sin menoscabo de la calidad en sus productos.

### Conclusiones

Aún cuando todos los componentes del ciclo de inteligencia tienen gran importancia, la diseminación o explotación de la misma en la relación productores – consumidores es crucial para cerrar el ciclo y garantizar que los productos generados cumplan con sus objetivos.

La relación entre consumidores y productores requiere un proceso de aprendizaje mutuo y reconstrucción permanente de capacidades, en las que los procesos de comunicación son fundamentales para el proceso de modernización y profesionalización en la gestión de los servicios de inteligencia.

**Manuel I. Balcázar Villarreal** fue Director General Adjunto de Seguridad Nacional en la Presidencia de la República (México).

### Entre el Temor y la Necesidad— un Ensayo de Interpretación Histórica

Jorge L. Jouroff

#### La necesidad de la información

El proceso mundial de globalización, que no supone el fin de la historia sino su continuidad, plantea los mismos problemas de antaño pero de otra forma y a nivel mundial. La llamada revolución en la información, en particular el uso de internet, han masificado el acceso a la información y aumentado la cantidad disponible a nivel público en forma exponencial.

La avalancha de datos y la necesidad de comprender el mundo imponen entonces las dos premisas fundamentales: la calidad de la información, es decir, saber seleccionar de entre la cantidad de datos los relevantes al asunto en cuestión, y, como siempre, la metodología del análisis, el marco conceptual.

Con las nuevas tecnologías de la información, los datos abundan, pero es necesario saber leerlos, como en cualquier ciencia. La comprensión del proceso global, el análisis, es lo que transforma la información en inteligencia y a su vez, en un insumo clave para la toma de decisiones y la conducción del Estado. Es la propia complejidad del proceso lo que va evidenciando la necesidad de dejar de lado la práctica de tomar decisiones basadas en la intuición -o las supuestas “verdades evidentes”- mas que en el conocimiento propiamente dicho.

De ahí la importancia de *la inteligencia estratégica*, con sus variantes.<sup>311</sup> Como toda inteligencia, ésta supone también la acumulación, sistematización y gestión del conocimiento. Una tarea que no puede ser sólo de un gobierno, sino que necesariamente debe abarcar un período bastante más prolongado, y por tanto, la estabilidad de un sistema. La estabilidad siempre ha sido un concepto relativo hablando en períodos históricos, pero es estabilidad al fin. Por ello supone ciertos consensos políticos.

#### La gestión del conocimiento

Como vemos, hay más de un equilibrio. Si partimos de la base que el gobierno no sólo debe gestionar sino fundamentalmente conducir, entonces,



es ineludible el conocimiento de esa marcha objetiva del proceso social. La producción de conocimiento científico, supone no sólo la recolección de datos y su análisis, sino su interpretación, a través de un ordenamiento que nos permita comprender el mundo en que vivimos. De esa forma es que podemos predecir *las tendencias posibles* del desarrollo, y a través de la gestión, conducir de la manera más adecuada posible.

Nuevamente debemos volver a la tarea sistemática, prolongada, paciente, de recopilación y análisis para comprender el valor de la inteligencia estratégica *como una forma de producción del conocimiento*. De ahí su valor como asesoramiento no al gobierno de turno, sino al gobierno del país.

### El sistema democrático de gobierno

La gestión en el sistema democrático, por lo anterior, debe cuidar también un determinado equilibrio entre los poderes, como propia garantía del mismo. El manejo del poder tras bambalinas y los secretos en la toma de decisiones predominaban en la época de los Imperios. La inteligencia, naciente, no escapaba a ello. Actualmente, es necesaria una mayor transparencia y control civil, como bases de la confianza a nivel político e institucional.

Y surge la eterna pregunta: ¿Quién controla a los controladores?

Una respuesta posible puede ser el auto-control mediante una perspectiva ética por parte de los practicantes, derivada de la educación y la responsabilidad que impone la autonomía de decisión dentro de los servicios especializados de información e inteligencia. Esta posibilidad se ha ensayado muchas veces, con escaso éxito, como muestra la historia.

Otra posible respuesta es el fortalecimiento de los controles institucionales. Desde el propio poder ejecutivo, con controles de otros organismos, externos, al control Legislativo, la supervisión (un término quizás más adecuado que control) intenta establecer un equilibrio entre las necesidades del gobierno y las necesarias garantías. Expresa, además, el necesario convencimiento que dichos organismos estarán al servicio del gobierno y la sociedad y no del gobierno de turno.

Entendamos que no hay garantías absolutas. Pero sí se observa el principio que para supervisar hay que conocer, y, en un orden democrático, quien supervisa

## Gestión de Inteligencia en las Américas

debe conocer. Existe un delicado equilibrio entre el secreto necesario -a veces- y las garantías democráticas.

Implica, también, estabilidad en el sistema democrático mismo, y el convencimiento de los actores de la propia estabilidad. De esa forma, aunque siempre permanecerá la necesidad de la supervisión y el mantenimiento de los equilibrios, la necesidad podrá prevalecer sobre el temor, siempre y cuando seamos capaces de construir organismos eficaces a la labor del gobierno y el Estado.

En América Latina será necesario superar además el justificado temor a la autonomización de dichos organismos, dado su rol en la represión y las dictaduras del Cono Sur en la segunda mitad del siglo pasado. Pero también es necesario recordar que dichas situaciones se produjeron fundamentalmente por decisiones políticas, y no porque los organismos se hubieren “desbordado” o “autonomizado”, aunque ese riesgo siempre exista. Hablamos de decisiones que se tomaron en la esfera de la conducción política (primero civil y luego, por supuesto, militar, pero en calidad de conducción.)

Es en ese sentido que el compromiso democrático debe prevalecer y establecer los controles y garantías necesarios para el propio sistema a la vez que rediseña o crea los organismos necesarios para proveer al gobierno de la necesaria inteligencia estratégica.

### Breves comentarios sobre los temas relevantes

La presente obra constituye un enorme esfuerzo en ese sentido: intenta contribuir tanto a la divulgación como al necesario debate sobre estos temas, sin los tabúes de antaño. Completa las dos anteriores sobre profesionalismo y democratización de la inteligencia.<sup>312</sup>

Los ensayos del presente capítulo, en conjunto, intentan mostrar un panorama del desarrollo de la gestión de los organismos de inteligencia, así como de determinados problemas relacionados, y la gama de sus resoluciones, logrando, además cubrir un panorama mayor que la propia nacionalidad de los autores.

### La inteligencia estratégica

El argentino Mariano Bartolomé comienza con una observación fundamental: con alguna excepción, no existe producción de inteligencia estratégica

propiamente dicha en el Cono Sur. Luego de definir acertadamente los períodos dictatoriales en América del Sur, en los cuales no había producción de inteligencia, salvo la operativa, repasa los casos más relevantes del período actual y concluye con la escasa o nula producción de verdadera inteligencia estratégica. Ello no supone que no existan personas capacitadas en los servicios de inteligencia, y pone varios ejemplos, pero no es aprovechada por el Estado como un sistema, y sobre todo, para la toma de las decisiones a nivel de conducción política.

El problema empieza con la misma definición de “inteligencia estratégica”, donde el autor comprende tres acepciones:

¿Qué es lo que define como “estratégica” a la inteligencia? Desde el punto de vista del autor, en base a la experiencia del caso argentino, suele adjetivarse como estratégica a la actividad de inteligencia en tres situaciones diferentes. En primer término, cuando su producto se basa en insumos proporcionados por otros organismos o agencias (por ejemplo, órganos militares); en este caso, el organismo encargado de la elaboración de inteligencia estratégica carece de medios de reunión de información propios, sino que se nutre de la inteligencia confeccionada previamente por las instituciones que integran el sistema o comunidad, según sea el caso. Segundo, cuando el producto pretende apuntar al mediano y largo plazos; y en tercer lugar, cuando el producto es particularmente importante o relevante. En este trabajo, entendemos que la inteligencia estratégica es el producto de inteligencia para empleo del máximo poder decisorio, que trasciende a la inmediatez y la coyuntura para identificar en relación al Estado, con un horizonte temporal mayor, tanto amenazas reales o potenciales, como oportunidades.

A nuestro entender, de la misma forma que en estrategia el carácter de la tarea determina su clasificación, y no los medios empleados, la sola mención de “estratégica” nos lleva a pensar en los objetivos más relevantes (que hacen a la propia naturaleza del Estado), y, por ello mismo, a mediano o largo plazo. Dado que refiere a la conducción del Estado, *reviste el carácter de asesoría* al más alto nivel, integrándose, de esa forma, al sistema democrático.

Ello fue (y es) particularmente notorio en Brasil, y desde hace ya cierto tiempo. Justo es reconocer que el desarrollo en ese país comenzó con la llamada “Escuela de la Sorbonne”, que dio escritores que pensaban el Brasil en términos

## Gestión de Inteligencia en las Américas

globales y de geopolítica, y lo proyectaban, notoriamente Travassos y los militares Golbery Da Couto e Silva y Meira Mattos, entre otros.<sup>313</sup> En el resto de América del Sur hubo intentos también en Argentina<sup>314</sup> y Chile, ésta última vinculada sobre todo al pensamiento naval, pero, a diferencia de Brasil, *no existía la potencialidad en la base material* que le diera viabilidad al proyecto. No por casualidad surgieron en períodos de ajuste del sistema mundial. Brasil, no sólo por sus características continentales, sino también por la persistencia en el proyecto, con la planificación y ductibilidad necesarias, logró integrar el corto con el mediano y largo plazo, desde el golpe de Estado de 1964 en adelante. Hoy es el país con mayor potencialidad de América del Sur, y, como bien señala el autor, desarrolló no sólo escuela sino también agencias a nivel estratégico.

Surge una interesante cuestión: si bien, como vimos, son los países con mayor tamaño y potencialidad los que han desarrollado inteligencia estratégica, ésta es necesaria por igual a todos, dada la integración al mercado mundial. De esa forma, países “pequeños”, como Paraguay y Uruguay, han hecho (y hacen) esfuerzos por remodelar los sectores de defensa e inteligencia. Ello se refleja en el siguiente parágrafo de Bartolomé:

La Inteligencia Estratégica constituye una herramienta fundamental en el marco de los esfuerzos que despliega el Estado moderno para prevenir, combatir y neutralizar las amenazas transnacionales que afectan a su sociedad y los ciudadanos que la integran. Acertadamente se ha dicho, en relación a tales amenazas, que “requerirán de una mejor comprensión, información y análisis, que sea entregada en forma oportuna y eficaz, para que los respectivos conductores políticos opten por las mejores decisiones”. Este rol ha sido resumido por Luís Alberto Sallaberry, en esa época titular de la ABIN brasileña, como una “asesoría estratégica” a la Presidencia de la República.

Este rol de “asesoría” subraya el hecho que la inteligencia estratégica es así concebida como fundamentalmente *analítica* y no operativa.

Resaltan, además, tres cuestiones: en primer lugar, no sólo qué inteligencia queremos, sino qué tipo de inteligencia tenemos posibilidades de desarrollar;

en segundo lugar, las formas organizativas con las que estructurar dicho sistema; y en tercer lugar: ¿Cuáles serían las probables áreas de análisis?

América Latina no dispone de recursos humanos adiestrados en abundancia, pero sí dispone de capacidad para desarrollar inteligencia humana, y estructurar la cooperación interagencial en lo interno como la cooperación regional de forma de optimizar los resultados.

La forma que adopte el sistema es más compleja; Bartolomé hace la observación exacta:

De todas maneras, la fisonomía que adopte la cooperación estará supeditada a la forma de estructuración de los organismos de inteligencia. ¿Constituyen estas agencias una comunidad donde la cabeza ejerce tareas de coordinación, o por el contrario conforman un sistema donde su cabeza ejerce una función de control?

Hemos remarcado que la mayoría de las veces existen varias agencias de inteligencia, pero no un sistema o una comunidad, pues éste último supone no sólo la mera existencia de un grupo de agencias, sino su coordinación y complementariedad, y la interconexión de las partes. Supone, por tanto, un plan de recolección de inteligencia a nivel nacional, acorde a las prioridades definidas.

Uno de los aspectos importantes a resolver es si el sistema se constituye manteniendo la coordinación entre las distintas agencias o si la coordinación comienza a adquirir un rol más activo en la conducción del sistema, transformándose de coordinación en un órgano rector. En ese sentido se están discutiendo en nuestros países, a nivel parlamentario, las alternativas y lo que implican cada una de ellas.<sup>315</sup> El rediseño también puede implicar las áreas de seguridad y defensa, por tanto, hay casos que los cambios afectan a varios sectores, y con ellos, a las agencias que existen en su órbita, redefiniendo los perfiles y las dependencias.

El ensayo de Álvaro Venegas, colombiano, nos ilustra sobre la inteligencia económica gubernamental, que se entiende como “el conocimiento resultante de un plan de búsqueda, reunión, evaluación, difusión y protección de información relacionada con fenómenos y actores económicos nacionales

## Gestión de Inteligencia en las Américas

e internacionales, que representen un desafío o una oportunidad para los intereses nacionales”. Expresamente lo distingue del espionaje económico, al formar equipos de análisis a nivel gubernamental, como forma de contribuir a la toma de decisiones a ese nivel.

Vincula el ciclo clásico de inteligencia: recopilación-análisis-difusión, con la teoría de Sims, que, además, incluye las funciones de anticipación y manipulación (contrainteligencia), a fin de anticiparse y debilitar al adversario. En palabras del autor, la teoría de Sims “ofrece un medio sistemático y medible del éxito en determinadas actividades, para evaluar un estudio de caso en su aplicación”.

Aparece aquí su utilidad, en tanto sea comprendida así por los gobiernos, destinatarios de la información. En este sentido, la producción de inteligencia ya no se limita al clásico concepto de amenaza, sino que, a través del método, pretende contribuir en áreas claves como la economía, percibiendo oportunidades y dibujando posibles escenarios.

El tema de los recursos descrito con sobriedad y precisión por Dan Elkins, demuestra un enfoque pragmático y experiente del tema. Con dos precisiones: se refiere a un sistema, sofisticado, como el sistema de inteligencia norteamericano, que no tiene par en América Latina, ni por los recursos, ni por la extensión de los medios que dispone. En ese sentido, maneja conceptos propios de esa realidad. Sin embargo, valen las generales de la ley: al presupuesto, *concebido como la expresión numérica de la política, se agrega el tema de la gestión* de los recursos mismos. Segundo, maneja un concepto “clientelar” en cuanto a los resultados, no siempre válido en estas latitudes.

Si somos capaces no de copiar el método, sino de adaptarlo, nos da una serie de lecciones; para comenzar, identifica cuatro niveles de interés gubernamental en el tema, nombrados por el brasileño Gonçalves, en su ensayo de la primera sección del presente libro: 1) agencia-interno, dentro de una agencia de inteligencia en particular; 2) ejecutiva-realizado por dentro de la rama ejecutiva por entidades de la administración que no se tratan de inteligencia y por el Departamento o Ministerio en que se pertenece la agencia de inteligencia; 3) externo-ejercido por la rama judicial, por la rama legislativa, y/o por una entidad independiente; y 4) popular-donde se aplican los intereses de ciudadanos individuales u organizaciones de la sociedad civil.

Es decir, dos niveles dentro del ejecutivo, dentro de la propia agencia y otro por fuera de ésta; un tercero, que en nuestro caso estaría referido más al control parlamentario que judicial, y un cuarto que denomina “popular”.

Un aporte adicional es la distinción entre eficacia y eficiencia: usualmente, estamos acostumbrados a medir los éxitos en el resultado de las misiones, más allá de los costos necesarios para lograrlo. Al respecto, a través de criterios de mensuración; propone una serie de preguntas que pueden servir como indicadores en los dos sentidos: el éxito operativo y el manejo presupuestal, entendiendo por eficacia al primero y definiendo al segundo (eficiencia) como el uso racional y óptimo, en sentido económico, de los recursos asignados. La lección es que el punto de vista económico es tarea fundamental para la continuidad de la tarea.

El ensayo finaliza con una serie de recomendaciones prácticas, abarcando de este modo el ciclo completo: definiciones básicas, criterios de medición, definición de metas, criterios de evaluación. Es importante estudiar el tema, además, puesto que en nuestra región se está comenzando a conformar un sistema de inteligencia, y la experiencia ajena nos puede permitir avanzar más velozmente en este sentido.

Para finalizar, la chilena Carolina Sancho en una investigación abarcativa, nos plantea la importancia de la cooperación en materia de inteligencia, en particular en UNASUR. Aquí, la primera dificultad viene dada por las propias estructuras nacionales, que no son homogéneas ni tienen los mismos cometidos en los distintos países; no obstante, la necesidad de la cooperación se impone por dos causas: por un lado, la creciente globalización, que obliga a aunar fuerzas, y por otro, casi como consecuencia, las amenazas o desafíos comunes.

Debido a esa contradicción entre los intereses comunes frente a la globalización y los intereses propiamente nacionales, es que la cooperación puede -y debe- ser muy amplia pero nunca absoluta (ilimitada, como dice la autora), entendiendo por cooperación no sólo el intercambio de información sino la capacidad de trabajar en conjunto en aras de los intereses comunes.

Está sobreentendido que dicha cooperación *presupone* pactos y alianzas políticas regionales que, en el marco de los gobiernos democráticos, posibiliten y hagan viable dicha cooperación. Esto se manifiesta en “la convergencia de

## Gestión de Inteligencia en las Américas

las políticas de seguridad, defensa y relaciones exteriores, como también, homogeneidad en los niveles de seguridad de las agencias y la capacidad de sus funcionarios”.

Cabe destacar los pactos regionales, los bilaterales, y los acuerdos surgidos de los organismos internacionales, puntuales, que a menudo se superponen. En América Latina existen dos grandes alianzas regionales: el Mercado Común del Sur (MERCOSUR) y la Comunidad Andina de Naciones (CAN).

Reseñando el caso de la Unión Europea, pasa luego al MERCOSUR, destacando cooperación en el ámbito de la inteligencia criminal las Reuniones de Ministros del Interior del Mercosur (la autora distingue también la cooperación antiterrorista). Destaca como herramientas perfectibles AMERIPOL y CLACIP, aunque señala que no tienen control político.

En materia de defensa, si bien es cierto que no existen aún herramientas institucionalizadas a nivel de subregión de cooperación en materia de inteligencia de defensa o de inteligencia estratégica nacional externa, pensamos que la UNASUR ahora constituye un primer paso en este sentido.

Se note que sí existe la Red Sudamericana de Comunicaciones Protegidas (SURNET), dirigida por el Comando Sur de Estados Unidos como posible base de cooperación en inteligencia. Además, en el ámbito de la inteligencia financiera, destaca el Grupo de Acción Financiera Sudamericana (GAFISUD) y la Oficina Regional de Enlace de Inteligencia (RILO), en la cooperación de información de aduanas.

Si vamos más allá de lo estrictamente puntual, vemos que, desde fines de la mitad del siglo pasado, ha habido un proceso continuo de salida de las dictaduras, afianzamiento de los sistemas democráticos, e, impelidos por los intereses comunes y la creciente globalización, un proceso de construcción de mecanismos regionales de defensa de esos mismos intereses comunes.

En Europa ese proceso, sobre la base del fin de la segunda guerra mundial y tratándose de potencias capitalistas desarrolladas, lleva mucho más tiempo que en nuestro continente, debiendo readecuarse continuamente a las nuevas realidades. Uniones aduaneras, complementación industrial, proyectos industriales comunes, en el marco de una alianza europea con la potencia



dominante (la OTAN) que ya enmarcaba las políticas de defensa, *y por tanto*, de cooperación en inteligencia, todo se mantuvo pese a las variadas reformulaciones de sus misiones, justamente porque se mantenía vigente la idea de una Europa unida.

El proceso en América Latina tiene similitudes y diferencias: son países periféricos, no centrales, en términos políticos y económicos, pero con una cada vez mayor integración al mercado mundial, y, por tanto, pese a las diferencias históricas, con una mayor conciencia de ello y de la defensa de sus intereses, *a la vez que* de la complementariedad con la economía mundial. Ese proceso ha llevado a la creación de los mecanismos actuales, perfectibles, y seguramente llevará a la creación de otros, pero lo importante es que el proceso que comenzó con pactos bilaterales, luego MERCOSUR y luego, en defensa, el más reciente UNASUR, es estable y está en construcción. Es lógico también que se superpongan los tratados y organismos bilaterales y aún regionales ya existentes, y seguramente coexistirán por un largo período, pues expresan herramientas de alianzas que también siguen vigentes.

Por último, vale la pena volver al inicio, y reconocer que el desarrollo desigual dificulta el avance en la materia, pero la conciencia en los objetivos comunes *y la irreversibilidad del proceso de globalización* nos debería impulsar a persistir en la conformación de los organismos de información comunes.

## Gestión de Inteligencia en las Américas

**Jorge L. Jouroff** cursó estudios de Ciencias Económicas en la Facultad de Ciencias Económicas y de Historia en la Facultad de Humanidades y Ciencias, Universidad de la República. Ha publicado *Seguridad Pública y Derechos Humanos*, Ediciones de la Banda Oriental, Montevideo, marzo del 2005. Su ensayo sobre el sistema de inteligencia de Uruguay, “Inteligencia y cultura: Una propuesta para Uruguay”, fue publicado por la National Defense Intelligence College, Washington, en 2009.

Se ha desempeñado como representante partidario ante la Comisión Central de Programa del Frente Amplio; miembro pleno de las Comisiones de Defensa Nacional y de Seguridad Ciudadana, asesor en temas de la especialidad a nivel de la bancada parlamentaria. Ha sido Director General de Secretaría del Ministerio del Interior (ROU) y se desempeñó en Presidencia de la República, en el Sistema Nacional de Emergencias, como asesor del Programa de Naciones Unidas de Desarrollo. También se desempeñó como Gerente General del SEMEJI (sistema de medidas para jóvenes en infracción). Actualmente se desempeña como profesor en la Escuela Policial de Estudios Superiores y, en el área privada, como consultor. Mails de contacto: admijor@adinet.com.uy y jorgejou@yahoo.com.



## La Inteligencia Estratégica y Sus Requisitos para la Seguridad en América del Sur

Mariano Bartolomé

### Introducción

En América del Sur, la cuestión de la inteligencia nacional no sólo no ocupa espacios relevantes dentro de la producción científica local, sino que su presencia en ese ámbito es escasa en el mejor de los casos, y nula en el peor. Específicamente en el país de origen del autor del presente trabajo, con la notable excepción de la obra de Ugarte, los escasos trabajos académicos existentes remiten a enfoques policiales o a lecturas empresariales y de administración de negocios.<sup>316</sup> A la hora de explorar las causas de ese estado de cosas, aparece como una primera razón el desconocimiento que existe en la ciudadanía sobre lo que la inteligencia significa, facilitando que en el imaginario colectivo se instalen percepciones que normalmente suelen estar alejadas de la realidad.

Esas imágenes suelen tipificar a los organismos estatales de inteligencia como instrumentos a través de los cuales los regímenes autoritarios que signaron a la subregión hasta la década del 80, perpetraron violaciones y atropellos a los derechos civiles y las libertades individuales de los ciudadanos.

Los procesos de democratización que se iniciaron en América del Sur hace tres décadas y su progresiva consolidación desde ese momento hasta el presente, facilitaron el control civil sobre los organismos de inteligencia, incluyendo la formación de especialistas en la materia y el diseño de una carrera profesional para aquellos que se desempeñarán como funcionarios estatales. Sin embargo, no siempre se logró la instauración de una cultura política que sustente el legítimo rol de la inteligencia en una democracia, precondition esencial para lograr que el mencionado control civil sea pleno y efectivo.<sup>317</sup>

Por esa causa, a pesar de la consolidación de la democracia en el espacio sudamericano, en algunos sectores de las sociedades de los países que lo integran persisten las distorsiones sobre la inteligencia, asociándola a organismos que emplean de manera irrestricta los recursos (humanos, materiales, financieros) públicos con metas asociadas más a objetivos puntuales del gobierno de turno que a intereses nacionales, y que suelen estar exentos de las prácticas

de control y *accountability* características de una democracia sana, o sencillamente no las cumplen con el pretexto de poner en riesgo la eficiencia de sus actividades.<sup>318</sup>

Esporádicamente salen a la luz episodios que alimentan ese tipo de percepciones. Sólo por citar algunos ejemplos, en Brasil la situación se planteó cuando se imputó a la Agencia Brasileña de Informaciones (ABIN) de efectuar escuchas telefónicas no autorizadas por la justicia al presidente y los miembros del Supremo Tribunal Federal (STF), la máxima instancia judicial del país.<sup>319</sup>

En Venezuela se acusó al Servicio Bolivariano de Inteligencia Nacional (SEBIN), creado en junio de 2010, de amedrentar y hostigar a eurodiputados que se habían trasladado a esa nación caribeña a monitorear la transparencia de los comicios y el respeto a la libertad de expresión para medios de comunicación no alineados con el gobierno.<sup>320</sup> También se indica que el SEBIN, bajo manejo y supervisión de especialistas cubanos, intercepta los correos electrónicos de miles de venezolanos en su país y en Miami; una parte significativa de los correos intervenidos pertenecería a activistas, periodistas, militares, diplomáticos venezolanos en el extranjero y conocidos líderes de oposición.<sup>321</sup>

Pero el caso de mayor trascendencia tuvo lugar en Colombia, cuando se comprobó judicialmente que el Departamento Administrativo de Seguridad (DAS) realizaba tareas de espionaje interno sobre decenas de congresistas de los opositores Polo Democrático y Partido Liberal, dirigentes políticos, magistrados y líderes de entidades de la sociedad civil. Las actividades del organismo incluyeron interceptaciones de comunicaciones (las llamadas “chuzadas”), seguimientos e infiltraciones, y motivaron que tres ex jefes del Departamento fueran procesados por espionaje interno, uno de los cuales fue condenado a 25 años de cárcel.<sup>322</sup>

Frente a esta percepción que resulta de una negativa mezcla de desconocimiento y preconceptos, entendemos que conviene establecer los límites y alcances del concepto inteligencia. Concebida como una actividad, hace ya más de una década la definimos como “aquella que brinda información procesada, útil y oportuna, sobre alguna situación específica y que contribuye a optimizar el proceso de toma de decisiones”. Dicho de otro modo, la actividad de inteligencia provee al usuario no sólo de información, sino también de un *insight* específico

## Gestión de Inteligencia en las Américas

que le permite reducir los niveles de incertidumbre, facilitando el citado proceso decisorio.<sup>323</sup>

La referencia al “procesamiento”, por su parte, indica el fuerte sesgo cualitativo de esta disciplina, en tanto hace referencia a una acción específica de agregación y tratamiento analítico en una pirámide informacional, formada en la base por datos brutos y, en el vértice, por conocimientos reflexivos.<sup>324</sup>

En líneas generales, en la medida en que el proceso antes descrito alude a la acción de gobierno se hace referencia a la *inteligencia nacional o inteligencia de Estado*, cuestión sobre la cual no existen mayores discusiones semánticas en los marcos normativos y doctrinarios sudamericanos. Sin embargo, las certezas tienden a desdibujarse al momento de hablar de *inteligencia estratégica*, concepto sobre el cual no se observan consensos.

En este punto resulta imprescindible señalar la extrema heterogeneidad que se observa en América del Sur en lo que se refiere a las actividades estatales de inteligencia. De manera similar a lo que se registra en los campos de la Defensa y la Seguridad, en materia de inteligencia las naciones sudamericanas muestran importantes diferencias tanto orgánicas como funcionales. Las múltiples diferencias alcanzan, entre otras cuestiones, las atribuciones de los organismos (incluyendo la cuestión de las facultades policiales); su control por parte del poder legislativo; su relación con el poder judicial en términos de ejecución de actividades intrusivas; y la participación militar en actividades de inteligencia en el marco interno.<sup>325</sup>

¿Qué es lo que define como “estratégica” a la inteligencia? Desde el punto de vista del autor, en base a la experiencia del caso argentino,<sup>326</sup> suele adjetivarse como estratégica a la actividad de inteligencia en tres situaciones diferentes. En primer término, cuando su producto se basa en insumos proporcionados por otros organismos o agencias (por ejemplo, órganos militares); en este caso, el organismo encargado de la elaboración de inteligencia estratégica carece de medios de reunión de información propios, sino que se nutre de la inteligencia confeccionada previamente por las instituciones que integran el sistema o comunidad, según sea el caso. Segundo, cuando el producto pretende apuntar al mediano y largo plazos; y en tercer lugar, cuando el producto es particularmente importante o relevante. En este trabajo, entendemos que la inteligencia estratégica es el producto de inteligencia para empleo del máximo

poder decisorio, que trasciende a la inmediatez y la coyuntura para identificar en relación al Estado, con un horizonte temporal mayor, tanto amenazas reales o potenciales, como oportunidades.<sup>327</sup>

Debido a esta situación de pluralidad y diversidad de enfoques, no todos los países sudamericanos llevan adelante tareas de inteligencia estratégica. Quienes efectivamente lo hacen, en tanto, no necesariamente lo efectúan con esa denominación y las instituciones encargadas de elaborar ese producto exhiben notorias diferencias entre sí.

En definitiva, las particularidades que se observan en relación a la inteligencia estratégica en América del Sur influyen en el sesgo prescriptivo que tendrá el presente trabajo, que pretende responder a la siguiente pregunta: ¿cuáles son los requisitos que deben cumplir las labores de inteligencia estratégica que desarrollan o deben desarrollar las naciones sudamericanas?

### El dinámico escenario de seguridad de América del Sur

En materia de seguridad América del Sur muestra un escenario que se presenta como contradictorio, según cuál sea la lente con el cual se lo analice. Desde un punto de vista tradicional, de clara raíz westfaliana, en el cual las cuestiones de seguridad se enmarcan en dialécticas interestatales y se expresan clave militar, soslayando la naturaleza multidimensional del fenómeno, la realidad sudamericana es verdaderamente excepcional. Sin embargo, la situación es mucho menos placentera cuando se aborda la seguridad en términos no convencionales.

Las amenazas no convencionales a la seguridad reconocen apenas tres regularidades: sus protagonistas son actores no estatales; no siempre emplean la violencia como herramienta racional de política y, en caso de usarla, lo hacen fuera de los formatos tradicionales asociados a la lógica clausewitziana, incursionando en lo que usualmente se conoce como asimetría. Más allá de esos tres elementos, esta esfera se caracteriza por su heterogeneidad, que se incrementa por diferentes procesos de *securitización*,<sup>328</sup> dando lugar a una situación que fue simbólicamente definida como “incertidumbre estratégica” o “mundialización del miedo”.<sup>329</sup> Es decir, una permanente percepción de inseguridad que alcanza a todos los individuos, sin que puedan evitarlo, en la cual los peligros y amenazas no reconocen una fuente clara ni limitaciones territoriales o políticas a su accionar.

## Gestión de Inteligencia en las Américas

Dentro de la agenda no convencional de la seguridad se insertan las amenazas transnacionales. Tanto por sus dimensiones como por su complejidad, en América del Sur se destacan el terrorismo y la criminalidad organizada, que se vinculan con “áreas grises” funcionales a esos dos fenómenos.

Por ejemplo, se destaca la organización peruana Sendero Luminoso (SL), que viró del terrorismo al narcotráfico y a mediados de la década pasada, retomó las acciones armadas en el Valle de los Ríos Apurímac y Ene (VRAE) y extendió sus actividades más allá de Perú, confirmando su transnacionalidad. Así, comenzó a practicar robos a bancos en Bolivia y a vender droga en barrios de clase baja de la ciudad de Buenos Aires.<sup>330</sup>

Otro caso que debe mencionarse es el de las Fuerzas Armadas Revolucionarias de Colombia (FARC), abundando las evidencias del nivel de complejidad y transnacionalidad que alcanzaron sus acciones criminales. Esas constancias se incrementaron dramáticamente a partir de la información obtenida de los computadores personales de Raúl Reyes, encontrados en el campamento de Angostura donde fue abatido ese jefe insurgente en marzo del año 2008, en el marco de la Operación Fénix.<sup>331</sup>

A estos formatos híbridos de narcoterrorismo se agregan un conjunto de entidades que han apelado a la violencia como metodología, aunque no quedan claras aún sus metas verdaderas ni su capacidad operativa. En este último renglón merecen mencionarse las Células Revolucionarias Brigada Mauricio Morales, de Chile; el Movimiento Revolucionario de Liberación Carapaica, de Venezuela; y sobre todo el Ejército Popular Paraguayo (EPP): un grupo que es fruto del reagrupamiento de antiguos miembros del Partido Patria Libre y, aunque se autodefine como revolucionario de principios marxistas-leninistas, sus actividades están claramente orientadas al lucro mediante la realización de secuestros extorsivos a importantes ganaderos.<sup>332</sup>

En cuanto a la criminalidad organizada, Sudamérica se encuentra plenamente inserta en los esquemas globales de esta amenaza transnacional cuyas dimensiones son verdaderamente enormes: Específicamente, el crimen organizado sudamericano no puede ser analizado ni comprendido sin tener en cuenta lo que ocurre en esta materia en el resto de América Latina, e inclusive todo el hemisferio.



Según datos de la OEA, la violencia criminal tiene en América Latina carácter “pandémico” y le cuesta a sus ciudadanos más de US\$ 16 mil millones anuales; por otro lado, la región tiene apenas el 8% de la población mundial, pero acapara más del 40% de los homicidios y casi el 70% de los secuestros extorsivos que se cometen en el planeta cada año.<sup>333</sup> De acuerdo a evaluaciones de una ONG especializada en violencia urbana, 24 de las 25 ciudades más violentas del mundo son latinoamericanas, con la única excepción de la estadounidense New Orleans en el vigésimo primer lugar. La lista la encabeza la hondureña San Pedro Sula con una tasa de homicidios superior a 159 casos cada 100 mil habitantes (159/00000), seguida por Ciudad Juárez en México con 148/00000.<sup>334</sup>

En América Latina se encuentran presentes diferentes manifestaciones de criminalidad, aunque no con igual intensidad. Nítidamente se destaca por su gravedad la producción y tráfico ilícitos de drogas. En este panorama, América del Sur juega un rol clave: sin tomar en cuenta volúmenes marginales de heroína y *cannabis*, el subcontinente es responsable por la totalidad de la cocaína que se produce a nivel mundial. En su último reporte anual, la UNODC consigna que la superficie dedicada a los cultivos ilegales asociados a esa droga ronda las 149 mil hectáreas. De ese total, el 41% corresponde a Colombia, un porcentaje levemente inferior a Perú y el 20% residual a Bolivia. La cocaína generada por esas tres naciones andinas constituye la punta de un iceberg de dimensiones globales. Aunque no se conoce con certeza el monto de estos ilícitos, la UNODC calcula esa cifra (sobre todo en base a promedios de los precios de comercialización minorista en diferentes mercados) entre US\$75 mil millones y US\$100 millones anuales.<sup>335</sup>

Este flagelo transnacional y la violencia que conlleva se expanden por toda América del Sur, adoptando en cada país diferentes fisonomías de acuerdo a las características y condiciones locales. Ya se ha hecho referencia a las FARC y SL, pero no pueden dejar de mencionarse las llamadas “Bandas Criminales Emergentes” (BACRIM) colombianas, ni alertar sobre el crecimiento de los carteles criminales de Brasil.

El gobierno de Colombia ha tipificado a las BACRIM como el nuevo enemigo armado del Estado. El narcotráfico es la piedra basal de las actividades de estas bandas, que hoy totalizan aproximadamente unos 7 mil efectivos, casi tantos como las FARC.<sup>336</sup> Los carteles criminales de Brasil, en tanto,

## Gestión de Inteligencia en las Américas

se asientan en los barrios de bajos recursos (*favelas*) de las ciudades más importantes del país; desde allí se dedican sobre todo al tráfico de drogas, y en forma subsidiaria a otros ilícitos como prostitución, juego clandestino, tráfico de armas, contrabando y extorsión. Debido a sus dimensiones y peligrosidad resaltan el *Primer Comando de la Capital* (PCC) en San Pablo, mientras en Río de Janeiro se destaca especialmente el *Comando Vermelho* (CV).

Además de la producción y comercialización de drogas, con especial énfasis en la cocaína, en América del Sur se registran otras importantes manifestaciones de la criminalidad organizada, de clara dinámica transnacional. En este sentido, el tráfico de armas desempeña un papel crucial. Se podría suponer que en la región de América Latina concentra casi la mitad de las armas ilegales en circulación a nivel global, si se toman por ciertas las estimaciones del Centro para la Información de Defensa (DIC) de Washington, quien las calculó en más de 80 millones.<sup>337</sup>

En América del Sur los flujos ilegales de armas muestran una alta heterogeneidad. En parte provienen de países europeos (sobre todo de su sector oriental) o de la extinta Unión Soviética, empleando en sentido inverso las rutas que se utilizan para traficar cocaína al Viejo Continente. Los puntos de ingreso son terminales portuarias de diferentes países sudamericanos (Brasil, Venezuela, Ecuador) y centroamericanos (Panamá y sobre todo Nicaragua). También proceden de los stocks militares y policiales de la región, sustraídas de sus arsenales, arrebatadas a sus usuarios o directamente vendidas por estos últimos.

El inventario de armas existentes en manos de los grupos terroristas y criminales que operan en América del Sur, producto de su tráfico y comercialización ilegales, es extremadamente variado. Incluye desde armas de puño y subametralladoras, hasta modernos lanzacohetes AT-4 *Saab Bofors* como los incautados a las FARC, pasando por diferentes fusiles de asalto cal. 5,56 mm y 7,62 mm, ametralladoras antiaéreas rusas MAG-30 y lanzacohetes RPG como los empleados por SL para derribar helicópteros militares. Las oportunas detenciones de los traficantes mundiales de armas Monzer al-Kassar y Viktor Bout, en 2007 y 2008 respectivamente, dejaron al descubierto cuáles serían los niveles que podría alcanzar este ilícito en América del Sur si no tuvieran efecto los mecanismos internacionales de detección e interdicción: lanzamisiles antiaéreos portátiles (MANPADs) de origen ruso *Strela-II* e *Igla*, en ambos casos a las FARC.<sup>338</sup>

Finalmente, en materia de tráfico de personas, aunque América del Sur ocupa un lugar marginal dentro de los principales flujos mundiales en esta materia, este flagelo se hace presente sobre todo en la forma de la trata de personas. Existen corrientes de trata de personas que se originan en América del Sur y se proyectan hacia América del Norte (EE.UU. y Canadá), Europa (sobre todo España, Italia y Francia) e incluso Asia (como es el caso de Japón y Corea).<sup>339</sup>

### La inteligencia estratégica frente al desafío de seguridad en América del Sur

El escenario descrito en las páginas anteriores afecta a las políticas públicas que las naciones sudamericanas llevan adelante en materia de inteligencia, tomando a la seguridad (en tanto *safety*) como demanda ciudadana, exigiendo una optimización de las labores de inteligencia estratégica, en caso de que ya existan, o su desarrollo en forma urgente, si no es de esa manera. La inteligencia estratégica constituye una herramienta fundamental en el marco de los esfuerzos que despliega el Estado moderno para prevenir,<sup>340</sup> combatir y neutralizar las amenazas transnacionales que afectan a su sociedad y los ciudadanos que la integran. Acertadamente se ha dicho, en relación a tales amenazas, que “requerirán de una mejor comprensión, información y análisis, que sea entregada en forma oportuna y eficaz, para que los respectivos conductores políticos opten por las mejores decisiones”.<sup>341</sup> Este rol ha sido resumido por Luís Alberto Sallaberry, en esa época titular de la ABIN brasileña, como una “asesoría estratégica” a la Presidencia de la República.<sup>342</sup>

En mayor o menor grado, diferentes naciones sudamericanas parecen encaminarse a la satisfacción de ese requisito clave como es contar con una adecuada inteligencia estratégica. Quienes no contaban con ese insumo han comenzado a dar los primeros pasos en ese sentido.

Una de esas naciones es Paraguay, donde hace un tiempo el presidente Lugo ordenó la modernización de la cartera de Defensa y la optimización de sus tareas, incluyendo la conformación de un organismo apto para elaborar inteligencia estratégica, del cual carecía el país. En línea con las directivas presidenciales, ese ministerio organizó por primera vez un curso de inteligencia para formar a efectivos militares afectados a las operaciones contra el EPP y grupos que se dedican al crimen organizado y tráfico ilegales que atentan contra la estabilidad y el desarrollo nacional. “El objetivo es preparar, capacitar

## Gestión de Inteligencia en las Américas

y especializar los recursos humanos necesarios para hacer frente a las amenazas emergentes”, expresó en la apertura del curso el director del Instituto de Altos Estudios Estratégicos (IAEE), general Lezcano Dávalos.<sup>343</sup>

Otro caso relevante es el uruguayo, donde la modernización alcanzó tanto al Estado Mayor de la Defensa (ESMADE), cargo creado por la Ley de Defensa Nacional promulgada a comienzos del año 2010, como a la Dirección Nacional de Información e Inteligencia (DNII), entidad más bien policial que depende del Ministerio de Interior. En el caso del ESMADÉ, su titular incluyó entre las funciones del organismo el alertar a las autoridades políticas sobre un conjunto de desafíos y nuevas amenazas a la integridad del Estado nacional, a través de una focalización de las actividades de la inteligencia (en clara referencia a la Dirección Nacional de Inteligencia del Estado, DINACIE, órgano creado en 1999 e inserto en ese ministerio). Entre otras cuestiones, mencionó específicamente el narcoterrorismo, las migraciones masivas de población, las epidemias, las agresiones al medio ambiente, el tráfico de órganos y personas, el estallido de conflictos generados por desigualdades sociales, el avance de la marginalidad, la circulación de armas, los movimientos de capital en los que se recurre a la informática, el traslado de residuos tóxicos, el terrorismo tecnológico y el espionaje en el mundo de la industria.<sup>344</sup>

Respecto a la DNII, su máximo responsable ha declarado que la misión básica del organismo a su cargo consiste en obtener información que, a través del proceso de análisis y prospectiva, pueda transformarse en inteligencia estratégica, descrita como un tipo de inteligencia cuya función consiste en identificar riesgos y amenazas a los derechos y libertades de los ciudadanos, la integridad del Estado y la estabilidad de las instituciones democráticas. En esta línea, la inteligencia estratégica elaborada por la Dirección debe contribuir al diseño de una estrategia gubernamental que minimice o evite aquellos riesgos que puedan perjudicar los intereses y la soberanía de Uruguay.<sup>345</sup> En este punto, se percibe un efecto colateral negativo de los esfuerzos que se llevan adelante en Uruguay para producir inteligencia estratégica: la duplicación de esa tarea, pues el titular de la DNII ha indicado que la institución a su cargo la elabora, mientras algunas lecturas establecen que esa función debe ser realizada por la DINACIE.<sup>346</sup>

No puede faltar, en esta referencia a los procesos que llevan adelante los Estados sudamericanos para dotarse de una inteligencia estratégica adecuada a las circunstancias, el caso de Colombia. Los escándalos de espionaje interno

que rodearon al DAS, mencionados al inicio del presente trabajo, culminaron en su disolución por parte del Presidente Juan Manuel Santos y la posterior constitución de una Dirección Nacional de Inteligencia (DNI, inicialmente denominada Agencia Nacional de Inteligencia, ANI). La Dirección es una entidad de carácter civil adscrita a la Presidencia de la República y, en contraste al antiguo DAS, sólo cumplirá con funciones de inteligencia y contrainteligencia, dejando amplio espacio para el desarrollo de una perspectiva estratégica sobre el tema. Las demás funciones del DAS pasarán a cargo de otras instituciones del Estado. Así, miles de funcionarios del antiguo organismo pasaron al Cuerpo Técnico de Investigaciones (CTI) de la Fiscalía; al ministerio de Interior (protección de personalidades); a la cartera de Relaciones Exteriores (control migratorio); y a la Policía Nacional.<sup>347</sup>

Resulta extremadamente difícil prescribir un modelo de inteligencia estratégica para los países sudamericanos, debido a la extrema heterogeneidad que se observa en materia de inteligencia en esta parte del continente. Sin embargo, tomando nota de esas diferencias, consignadas al principio del presente trabajo, desde nuestro punto de vista existen cuatro condiciones básicas que debe cumplir la inteligencia estratégica en América del Sur, para enfrentar de manera eficaz las amenazas transnacionales que caracterizan su escenario de seguridad.

1. En primer lugar, en lo relativo a las fuentes, la revalorización en la base de la pirámide informacional de las fuentes las humanas (HUMINT), que confirman su importancia crucial incluso en esta época en que los avances tecnológicos permiten un aumento de las inteligencias de señales e imágenes, principalmente satelital. Por un lado, existen limitaciones y condicionantes para la captación de señales u obtención de imágenes por medios tecnológicos que no son aplicables, o pueden ser superadas por fuentes humanas. Por otra parte las imágenes y señales obtenidas por medios tecnológicos, más allá de su valor, pueden resultar insuficientes a la hora de efectuar evaluaciones políticas, puesto que no tienen en cuenta el factor humano, la principal variable independiente en todo análisis de escala estratégica.

Como acertadamente sostiene un especialista peruano, la HUMINT suele constituir la mejor vía -cuando no la única- para obtener información sobre actores cuya instancia decisoria se restringe a un núcleo restringido de personas que desarrollan sus tareas en un contexto hermético y endogámico cuya penetración requiere considerables dosis de tiempo.<sup>348</sup>

## Gestión de Inteligencia en las Américas

Probablemente no existan mejores ejemplos de la importancia de contar con una adecuada HUMINT, complementada (pero nunca reemplazada) por sólidas inteligencias de señales e imágenes, que los que proporcionó en los últimos tiempos el gobierno colombiano en su combate a las FARC. Así lo demuestran las operaciones en las cuales fueron abatidos sus líderes Raúl Reyes (“Operación Fénix”, marzo de 2008), Jorge Briceño (“Operación Sodoma”, septiembre de 2010) y Alfonso Cano (“Operación Odiseo”, octubre de 2011), y rescatada una docena de rehenes del grupo, incluyendo la dirigente política y ex candidata presidencial Ingrid Betancourt (“Operación Jaque”, junio de 2008).

Tomando como ejemplo a la Operación Fénix, en forma independiente de sus aristas más controvertidas, vinculadas con la violación de la integridad territorial de otra nación, esa acción fue el fruto de una vasta y compleja operación de inteligencia. La reconstrucción de los hechos obliga a remontarse al mes de febrero del año anterior, cuando en el seno de la Policía Nacional se constituyeron siete grupos especiales que actuarían por separado y cuya misión era localizar a cada uno de los miembros del Secretariado de las FARC. Uno de esos equipos se trasladó a la selvática zona del Putumayo, lindera con Ecuador, donde solía detectarse esporádicamente a Reyes. Las pacientes labores de inteligencia desarrolladas en el lugar empezaron a dar resultados, cuando uno de los agentes encubiertos logró ganarse la confianza de un integrante del esquema de seguridad del jefe insurgente.

A lo largo del tiempo, a través de ese contacto se fue incrementando el conocimiento sobre las actividades y desplazamiento de Reyes y su estructura, hasta conocerse de antemano la inminente instalación de uno de sus campamentos del lado ecuatoriano de la frontera binacional. Por esa época los agentes colombianos también obtuvieron el número del teléfono satelital que usaba el guerrillero para sus comunicaciones, que comenzó a ser monitoreado. El desenlace de la operación es conocido: establecida con exactitud la ubicación del campamento, gracias al monitoreo telefónico, el mismo fue atacado por bombas láser arrojadas por aviones de la Fuerza Aérea, tras lo cual desembarcaron en el lugar comandos helitransportados del Ejército y policiales.<sup>349</sup>

2. En segundo término, para lidiar contra las amenazas transnacionales que se observan en América del Sur, una adecuada inteligencia estratégica debe enfatizar en la cuestión de la cooperación, en un doble plano: el interinstitucional,

o interagencial dentro de un mismo Estado, y el intergubernamental entre dos o más países, sea de manera directa o en el marco de organismos internacionales. En la primera de esas esferas, se ha alegado que la misma complejidad de las situaciones que deben analizar los organismos de inteligencia exige la articulación de respuestas interdisciplinarias donde todos sus agentes intercambien puntos de vista.<sup>350</sup> A esto se debe agregar que el debate e intercambio de apreciaciones y perspectivas contribuye a limitar las distorsiones que se pueden generar en un proceso de análisis, tales como apego a las visiones tradicionales o la adopción de posturas corporativas.<sup>351</sup>

De todas maneras, la fisonomía que adopte la cooperación estará supeditada a la forma de estructuración de los organismos de inteligencia. ¿Constituyen estas agencias una comunidad donde la cabeza ejerce tareas de coordinación, o por el contrario conforman un sistema donde su cabeza ejerce una función de control?<sup>352</sup> Y en caso de componer un sistema, su grado de centralización constituye una variable esencial.

En América del Sur se han llevado adelante en los últimos tiempos interesantes iniciativas que contribuyen directa o indirectamente a la profundización y optimización de la cooperación interagencial en materia de inteligencia. Tres ejemplos concretos pueden citarse en este sentido, correspondientes a Colombia, Ecuador y Uruguay.

En Uruguay durante la administración del Presidente Tabaré Vázquez se creó la figura de Coordinador Nacional de Inteligencia, dependiente de la Presidencia de la República, estableciéndose a través de un decreto que su titular se encuentra facultado para requerir apoyos y toda la información disponible que posean los organismos de inteligencia estatales.<sup>353</sup> En Ecuador una comisión *ad hoc* determinó en el año 2008 que la Dirección de Inteligencia del Comando Conjunto de las Fuerzas Armadas tenía grandes debilidades en materia de procesamiento y análisis estratégico de la inteligencia, debido a la falta de coordinación entre los subsistemas militares que lo integraban, justificando una profunda reforma llevada adelante al año siguiente que derivó en la creación de la Secretaría Nacional de Inteligencia (SENAIN).<sup>354</sup> Poco después en Colombia se creó, en base a la experiencia estadounidense, el Consejo de Seguridad Nacional, con dependencia directa del Presidente de la República y la función de coordinar las labores de los ministerios de Defensa, Relaciones Exteriores, e Interior y Justicia.<sup>355</sup>

## Gestión de Inteligencia en las Américas

Respecto al plano intergubernamental, desde el mismo momento en que toda amenaza transnacional excede las fronteras de un Estado para expandirse a dos o más unidades políticas, su tratamiento no puede limitarse a acciones unilaterales sino que debe trascenderlas para alcanzar entendimientos bi o multilaterales. En ambas opciones, la postura de los actores participantes puede variar, limitando sus objetivos a la reducción de los efectos de la amenaza sobre las propias sociedades (*glocalización*), o trascendiendo esa meta para apuntar a la neutralización de las causas últimas que la motivan (*globalización*).<sup>356</sup>

La lógica cooperativa en materia de Seguridad Internacional ha sido reafirmada por la Organización de las Naciones Unidas (ONU), indicando que un nuevo mecanismo de seguridad global debe descansar en tres pilares básicos: que las amenazas actuales no reconocen fronteras nacionales; que están interconectadas entre sí; y que deben ser enfrentadas simultáneamente en los planos estatal, regional y global. Así, ningún Estado puede sólo por sus propios esfuerzos tornarse invulnerable a las amenazas no convencionales actuales, protegiendo a su población y despreocupándose de la situación de sus vecinos, pues la responsabilidad de su seguridad es compartida con otros Estados.<sup>357</sup>

En el ámbito sudamericano, Perú constituye una muestra válida de la conducta a seguir en esta materia. Cuando comenzaron a incrementarse en el territorio de ese país las acciones de los carteles criminales de México, elevándose además su nivel de violencia, desde el poder ejecutivo local se promovió una mayor cooperación de inteligencia entre los organismos locales y sus contrapartes mexicanos.<sup>358</sup> Idénticos llamamientos se efectuaron en oportunidad de la realización en Lima de una Reunión de Jefes de Organismos Encargados de Combatir el Tráfico Ilícito de Drogas en América Latina y el Caribe (HONLEA); en esa ocasión el presidente peruano reclamó la articulación de mecanismos de cooperación entre los sistemas de inteligencias latinoamericanos, para combatir de manera eficaz la legalización de activos ilícitos procedentes del narcotráfico.<sup>359</sup>

El caso de la Triple Frontera merece ser citado como ejemplo concreto de una adecuada cooperación intergubernamental de tipo multilateral en materia de inteligencia estratégica en la región. Luego de los atentados terroristas de 1992 y 1994 se constituyó el llamado Comando Tripartito, integrado por Argentina, Brasil y Paraguay; con posterioridad se agregaron Uruguay y Chile en calidad de miembros invitados. Su objetivo esencial era aumentar y mejorar



la seguridad de esa zona geográfica a través de la cooperación de las fuerzas policiales y de seguridad de los tres países, en materias tales como narcotráfico y otras expresiones de crimen organizado; contrabando y falsificación; terrorismo; legalización de activos y tráfico de personas.

En el marco del Comando operó la llamada Mesa de Inteligencia, antecesora del posterior Centro Regional de Inteligencia (CRI). A través de ese sistema, los jefes locales de los organismos de inteligencia desplegados en el lugar compartían información sensitiva y coordinaban acciones encubiertas cuya meta era obligar a las organizaciones terroristas o criminales asentadas en la zona a desarticular sus redes/células y migrar hacia otras plazas, al verse obstaculizados sus negocios ilícitos.<sup>360</sup>

Simultáneamente a la constitución del Comando Tripartito, fueron montados una quincena de Unidades de Coordinación Conjunta (UCCs) en diferentes puntos fronterizos bilaterales entre Argentina, Paraguay, Brasil y, como incorporación novedosa, Uruguay. Las unidades están integradas por las fuerzas policiales y/o de seguridad desplegadas en el lugar, a ambos lados de la frontera, y sus jefes son quienes la coordinan. A semejanza de lo implementado en la Triple Frontera, las UCC sirven para el intercambio de información oportuna y confiable entre las partes, contribuyendo a la prevención y combate al crimen organizado y los delitos transfronterizos.<sup>361</sup>

Un lustro después de la constitución de la iniciativa de seguridad de los tres gobiernos, y sin duda bajo la influencia de los atentados del 11S, se constituyó el llamado Grupo 3 + 1 sobre Seguridad en Triple Frontera, sumándose EE.UU. como cuarto miembro (esta incorporación le agrega “globalidad” a una iniciativa que hasta el momento tenía un perfil “glocal”). Su finalidad consistió en intercambiar información sobre terrorismo y crimen organizado en la zona, compartir puntos de vista y perspectivas sobre la materia en un marco de confianza, y elaborar estrategias preventivas en estos aspectos.<sup>362</sup> Finalmente, en el marco de este Grupo en el año 2006 se puso en funciones el referido Centro Regional de Inteligencia (CRI), para incrementar los niveles de cooperación entre los cuatro países involucrados respecto a la provisión de inteligencia sobre la logística y financiación a grupos terroristas internacionales.

El esquema 3+1 vigente en la Triple Frontera, con participación de EE.UU, indica la importancia que reviste para las naciones sudamericanas la

## Gestión de Inteligencia en las Américas

cooperación con actores extrarregionales en materia de inteligencia, a través de mecanismos multilaterales. Más cerca en el tiempo, otro avance en esta materia se registró a mediados del año 2010, en ocasión de la V Cumbre de la Comunidad Latinoamericana y del Caribe de Inteligencia Policial.<sup>363</sup> En esa oportunidad el gobierno mexicano decidió compartir con las demás naciones latinoamericanas y caribeñas la llamada “Plataforma México”: una enorme base de datos que, entre otras cosas, alberga el Sistema Único de Información Criminal para todo el país. El objeto de la iniciativa fue optimizar la eficacia de la lucha contra el crimen organizado en el continente, teniendo en cuenta la expansión de los grupos aztecas hacia otras partes del continente.<sup>364</sup>

3. De cara a las amenazas transnacionales, la tercera condición básica que debe cumplir la inteligencia estratégica en América del Sur consiste en proporcionar a sus usuarios un producto de alta calidad, a tono con la complejidad de los tiempos que corren, cuyo empleo sea útil en los procesos de toma de decisiones. Ese uso, por otra parte, debe trascender el análisis del objeto de estudio y su evolución probable, para contribuir claramente al diseño de opciones alternativas realistas disponibles para el decisor.<sup>365</sup>

El salto cualitativo que plantea esta tercera condición se basa en las dos anteriores; es decir, tanto en una HUMINT en cantidad y calidad adecuadas, como en una sincera y fluida cooperación interagencial e intergubernamental. Pero también involucra otras cuestiones. Una de ellas es la renovada importancia de disciplinas y campos del conocimiento que en otras épocas tenían una jerarquía periférica, pero que hoy son imprescindibles para comprender de manera adecuada, manejar y prevenir las amenazas que deben enfrentarse.

En este sentido, los temas más importantes de la agenda de la Seguridad Internacional contemporánea, como los conflictos armados intraestatales y las amenazas transnacionales, entre ellas el terrorismo y la criminalidad organizada, se encuentran íntimamente vinculados con factores culturales que les dan sentido y un perfil propio e intransferible. Estos factores ayudan a evitar generalizaciones y estandarizaciones inapropiadas, y limitan la utilidad de las analogías históricas.<sup>366</sup> La antropología, la historia, el estudio de religiones comparadas y la sociología, entre otras áreas de conocimiento, protagonizan esa jerarquización.<sup>367</sup>

Otra cuestión a tener en cuenta en este punto apunta a la revalorización de los productos basados en fuentes abiertas (OSINT); en este sentido, la clave es incorporar al proceso de análisis un mayor caudal de información pública con alta especialización temática, con distintos formatos y diferentes procedencias. Dentro de la OSINT deben incluirse los llamados “*outsiders*”, personalidades con profundos conocimientos sobre una temática específica, que están en capacidad de proveer nuevos y valiosos puntos de vista a la estructura de inteligencia (además de contribuir a la limitación de las mencionadas distorsiones que pueden producirse en un proceso de análisis endogámico).

Un excelente ejemplo de elaboración de un producto analítico de alta calidad basado en HUMINT, cooperación interagencial, OSINT y *outsiders*, lo proporciona Colombia con su “Anuario Estadístico del Sector de la Defensa y la Seguridad 2003-2009”, elaborado por la cartera de Defensa como documento público de consulta sobre la lucha contra la criminalidad y el terrorismo durante ese período de siete años. El reporte también consigna cifras y tendencias en materia de delitos seleccionados (por ejemplo, secuestros), terrorismo, narcotráfico y otras formas de criminalidad organizada.

De acuerdo al ministerio de Defensa, el Anuario mejora el almacenamiento de datos, el diseño y aplicación de metodologías de análisis, el seguimiento y evaluación de las acciones de los actores estudiados y, sobre todo, el proceso de toma de decisiones dentro del sector y a nivel político. Además, facilita la interacción estatal con el mundo académico, facilitando su participación en el diseño de políticas públicas en materia de Seguridad y Defensa.<sup>368</sup>

4. La cuarta y última condición básica que debe cumplir la inteligencia estratégica sudamericana consiste en el desarrollo de una adecuada capacidad para identificar tendencias y diseñar escenarios de mediano y largo plazos sobre sus temas de interés, que trasciendan la coyuntura y el corto plazo.<sup>369</sup> Evaluaciones de este tipo, basadas en enfoques metodológicos predictivos o prospectivos, son elaboradas desde hace décadas por múltiples actores no estatales que han fluctuado entre informes reservados sobre cuestiones puntuales, y apreciaciones de nivel estratégico y carácter público. Esta prolífica tradición reconoce entre sus últimos exponentes a la obra “Los Próximos 100 Años”, donde el autor George Friedman elabora un escenario global para la segunda mitad del corriente siglo.<sup>370</sup>

## Gestión de Inteligencia en las Américas

Lejos de constituir un patrimonio reservado a académicos o empresarios, los estudios de mediano y largo plazos constituyen cada vez más un área de interés para la inteligencia estratégica, con el objeto de disminuir los márgenes de imprevisibilidad e incertidumbre que enfrentan los decisores. Una pauta en este sentido fue proporcionada hace pocos años por el Consejo Nacional de Inteligencia (NIC) de EEUU, un organismo gubernamental coordinado por el Director Nacional de Inteligencia cuyo objetivo es proporcionar análisis y evaluaciones sobre cuestiones internacionales al titular del poder ejecutivo y otros usuarios de máximo nivel. Hace pocos años el Consejo emitió el documento *Tendencias Globales 2015: Un Mundo Transformado* referido a la evolución de las principales cuestiones que hoy protagonizan al tablero internacional.<sup>371</sup>

Se ha postulado con acierto que, de cara a las amenazas no tradicionales a la seguridad que pesan sobre las sociedades latinoamericanas, la inteligencia estratégica juega un papel central llevando adelante análisis prospectivos que den “la voz de alarma” y contribuyan a la confección de planes de acción y contingencia.<sup>372</sup> En este sentido, las estimaciones de inteligencia a mediano y largo plazos constituyen insumos esenciales para el logro de acuerdos políticos que permitan la aplicación de políticas y estrategias estatales de Defensa y seguridad constantes y coherentes, más allá de los eventuales cambios de gobierno. Desde esta perspectiva, los mencionados acuerdos constituyen los pilares para una derrota definitiva de flagelos como el terrorismo y el narcotráfico.<sup>373</sup>

### Conclusiones finales

En las páginas precedentes hemos confirmado que en materia de seguridad, América del Sur presenta dos facetas claramente diferenciadas entre sí, según cuál sea el cristal a través del cual se analice su situación. Desde un enfoque tradicional, con una fuerte influencia teórica del realismo, que se concentra en las relaciones que se establecen entre actores estatales y realiza la dimensión militar del poder nacional, el espacio geográfico sudamericano muestra bajos niveles de conflictividad, la consolidación de una Zona de Paz y una creciente institucionalización cuyo mejor ejemplo es el Consejo de Defensa Sudamericano (CDS).<sup>374</sup>

En cambio, la realidad sudamericana en materia de seguridad se modifica drásticamente si nuestra perspectiva se aparta de la tradicional matriz westfaliana de conflicto entre Estados, para incursionar en el campo de las amenazas protagonizadas por actores no estatales que no siempre emplean la violencia

como herramienta racional de política, y de usarla, lo hacen en forma asimétrica. En este marco, se destacan por su peligrosidad y dimensiones dos amenazas transnacionales cuyo despliegue espacial aprovecha la existencia de áreas grises donde se observa una fragilización estatal y la caída de los niveles de gobernabilidad. Una de esas amenazas es el terrorismo, sea en un formato puro o degradado a partir de su reorientación hacia la criminalidad; la otra es precisamente el crimen organizado bajo la forma de los tráfico de drogas, armas y personas.

Frente a este panorama, resulta imperativo que las naciones de América del Sur desarrollen una adecuada inteligencia estratégica, entendida como un producto de inteligencia para empleo del máximo poder decisorio, que trasciende a la inmediatez y la coyuntura para identificar en relación al Estado, con un horizonte temporal mayor, tanto amenazas reales o potenciales, como oportunidades.

El alto grado de heterogeneidad que se observa en la región en materia de inteligencia torna extremadamente difícil la propuesta de un modelo concreto de inteligencia estratégica a adoptar por los países sudamericanos. No obstante, más allá de las diferencias, un combate eficaz contra las amenazas transnacionales exige que la inteligencia estratégica cumpla con cuatro condiciones básicas: en primer lugar, una adecuada valorización de las fuentes humanas (HUMINT), que no se vea afectada por el auge de otras formas de inteligencia más vinculadas con el avance tecnológico; segundo, fluidos niveles de cooperación interagencial e intergubernamental, en este caso respecto a cuestiones o áreas geográficas de interés común; en tercer término, la generación de un producto de alta calidad, apto para ser empleado en procesos de toma de decisiones; finalmente, la capacidad para identificar tendencias y diseñar escenarios de mediano y largo plazos, mediante el uso de metodologías predictivas o prospectivas.

Previsiblemente, el logro de estas cuatro condiciones demande importantes esfuerzos en dos niveles, el de la dirigencia política y el de los organismos de inteligencia, respectivamente. En el primer caso, sancionando modernas leyes de inteligencia que adecuen esta actividad a los tiempos presentes, disocien esta actividad de las tareas de corte represivo y establezcan adecuados mecanismos de control democrático y respeto a los derechos y libertades individuales. En el segundo, aplicando en las mencionadas instituciones profundos

## Gestión de Inteligencia en las Américas

cambios de paradigmas organizacionales, doctrina, formación y capacitación del personal, y relacionamiento con otros sectores de la sociedad, en especial el ámbito académico. Estos son los desafíos de los próximos tiempos.

### Biografía del autor

**Mariano Bartolomé:** Graduado y Doctor en Relaciones Internacionales (Universidad del Salvador, USAL). Master en Sociología (IVVVVE, Academia de Ciencias de la República Checa). Investigador Postdoctoral en Seguridad Internacional, Consejo Nacional de Investigaciones Científicas y Técnicas, CONICET). Profesor en la USAL, Universidad de Buenos Aires (UBA) y Universidad Nacional de Lanús (UNLa). Director del Posgrado en Políticas Públicas de Seguridad, Universidad de Morón (UM). Correo: marianobartolome@yahoo.com.ar.



## Gestión de Inteligencia Económica Gubernamental Una propuesta para examinar en el Área Andina

Álvaro José Venegas González

*Para los países occidentales la lucha contra el terror global necesitará librarse cada vez más en el terreno económico. Este es uno de los casos que requieren de una intervención estatal más grande y un papel más reducido del mercado y de los intereses creados.*

—George Magnus, economista senior  
Swiss Bank Corporation (UBS)

*El prudente ve el mal y se esconde, pero los ingenuos pasan y reciben el daño.*

—Proverbios 22:3

### El propósito

Este ensayo propone ampliar el alcance estratégico de la inteligencia en vista de cómo esta función del gobierno puede tratar con el juego de intereses económicos en contienda en el ámbito de seguridad interna y externa de cualquier Estado. Consideramos la creación de una entidad estratégica de inteligencia que vislumbre los desafíos económicos del Estado para posibilitar su supervivencia y aun la prosperidad en el sistema internacional. En la región andina, un Estado y su gobierno tiene interés por expandir y fortalecer su infraestructura energética e ideológica; el comercio ilícito y la captación ilegal de dinero, fenómeno y delitos de orden económico de impacto en la seguridad nacional de los países vecinos. Estos antecedentes acompañados de evidencias justificarían la evaluación y aplicación sistemática de la Teoría de Realismo Adaptativo, respecto de los procesos de inteligencia, para poder desarrollar una perspectiva económica estratégica apta para el más alto nivel decisional gubernamental.<sup>375</sup>

### El escenario

Por tomar apenas algunos testimonios de estudiosos en inteligencia y economía, existe la necesidad y no es para menos, prestar mayor atención a la vulnerabilidad de los gobiernos sobre los dramáticos cambios en los roles del



Estado-Nación y la inseparable transformación condicionada por el contexto económico internacional.

Si los banqueros y las finanzas internacionales están corroyendo a los Estados desde arriba; los terroristas y los traficantes de drogas retan el poder del Estado desde abajo, haciendo uso de la tecnología y de las redes internacionales que actúan alrededor y a través de los Estados, para buscar sus objetivos al tratar de exigir la aprobación o elusión del control estatal.<sup>376</sup>

La realidad estratégica de la inteligencia está inserta en lo que el almirante Pierre Lacoste llama el segundo mundo, donde “los problemas son más ambiguos que en el primero, las preocupaciones de seguridad exterior e interior están aún más estrechamente ligadas en el contexto de la universalidad, de la globalización y de la desregulación de las economías y por ende se torna cada vez más difícil establecer una distinción entre los intereses nacionales y los sectoriales”.<sup>377</sup>

Como en el caso anterior, el economista Moisés Naím,<sup>378</sup> afirma que las reformas para promover la economía de mercado durante la década de los 90, debilitó el control de los gobiernos sobre las fronteras y aumentaron los incentivos a las organizaciones criminales (pseudoempresas), dispuestas a erosionar las economías, aumentar su capacidad corruptora y socavar la autoridad de los Estados en los mercados ilícitos de armas, drogas, seres humanos, propiedad intelectual y dinero. Es por ello que el problema obedece a la frágil reacción del poder estatal para anticipar los planes y acciones de estos actores no estatales, cobijados en una zona gris de transacciones legales e ilegales.

Contribuyendo a enrarecer aún más el escenario, Carlos Lleras Restrepo, economista y expresidente colombiano, señalaba hace algo más de dos décadas “Tan graves o más graves que los actos terroristas de las guerrillas son los asaltos al patrimonio de los particulares y de las entidades públicas”,<sup>379</sup> de manera que es cada vez más cuestionable, como el país no ha estado preparado para prevenir oportunamente este flagelo.

De esta forma, Lacoste, Naím y Lleras colocan de manifiesto las debilidades y amenazas al Estado y en medio de semejante panorama ha de suponerse que los organismos de inteligencia gubernamental y de contrainteligencia no poseen la capacidad de abarcar la reunión, análisis y transmisión de perspectivas

## Gestión de Inteligencia en las Américas

“procesables” sobre el amplio campo de juego de intereses económicos. En tal caso, emerge la pregunta obedecida a un ambiente económico de globalización, privatización y liberalización ¿no sería mejor dejar esa labor al sector privado, que en su libertad de acción pueda atender el tema desde una perspectiva más especializada y dinámica?

Precisamente, si el auge y la consolidación de la inteligencia privada excede la capacidad de la comunidad de inteligencia, al orientar y mejorar la capacidad de acceso y procesamiento de información económica privilegiada de países con diferencias políticas y actores en competencia con poder desestabilizador; depender y delegar esta responsabilidad sería riesgoso para la seguridad nacional si no hay claridad en la frontera legal y la regulación del Estado, que evite la ilegalidad de éstos al obtener información sensitiva de utilidad para la defensa exclusiva de sus intereses privados.

En este contexto sobresale un argumento del país ibérico,

Por un lado, en relación con el desempeño de funciones que lindan o recaen dentro de lo "inherentemente gubernamental", aunque se admite, como regla general, que las empresas privadas no deben ser admitidas en el desempeño de este tipo de funciones, la práctica muestra, que el recurso al sector privado puede resultar imprescindible en algunos ámbitos.<sup>380</sup>

Una precisión adicional al planteamiento anterior, reside en la repercusión sobre cualquier acción crítica de contrainteligencia de proveedores privados, para reducir la capacidad de inteligencia de un servicio de inteligencia opositor, especialmente en el exterior, puede dar origen a la ruptura de relaciones entre países y, en el caso más extremo, hasta a una guerra armada que indebidamente involucre a toda una nación.

Justamente la inteligencia debe ser una herramienta competitiva que proteja los intereses nacionales en tiempos de escasez o abundancia, al favorecer las condiciones de seguridad en pro de un desarrollo y crecimiento. En concurso con el tejido económico representado en gremios con alta reputación y corporaciones socialmente responsables, que con su influencia en las políticas de los gobiernos, no favorezcan exclusivamente sus intereses en desmedro del fin supremo del Estado, el bien común.

De hecho, el empleo gubernamental de los funcionarios de inteligencia y expertos en economía, negocios y finanzas internacionales dependerá de si las respuestas son de aplicación práctica y reveladora, como resultado de hechos fiables de información abierta; acompañados de la recolección de información, la transmisión, la anticipación y la degradación de los esfuerzos de los oponentes (contrainteligencia), funciones críticas de la teoría del realismo adaptativo.

Tomando en cuenta la anterior intención ilustrativa, ¿Cuál sería el alcance y la doctrina de un equipo de trabajo oficial para contribuir al logro de los objetivos estratégicos de la Inteligencia Económica Gubernamental (IEcG)?

### Antecedentes de una perspectiva teórica

#### *La IEcG, una definición formal*

En el contexto gubernamental puede definirse y enfocarse la IEcG, como el conocimiento resultante de un plan de búsqueda, reunión, evaluación, difusión y protección de información relacionada con fenómenos y actores económicos nacionales e internacionales, que representen un desafío o una oportunidad para los intereses nacionales. Esto para diferenciarlo básicamente del espionaje económico, que por definición oficial es la actividad clandestina e ilegal llevada a cabo por un gobierno extranjero y/o una empresa privada, tendiente a obtener acceso a información privilegiada de la economía de un país, con el fin de obtener una ventaja económica.<sup>381</sup>

De tal manera, que sólo cuando se estudien casos e investigaciones reales de espionaje económico, en gran medida poco documentados, podría surgir un nuevo marco legislativo, el derecho penal del enemigo. Bajo esta denominación se hace referencia al derecho penal que trata a los infractores como enemigos, es decir, como meras fuentes de peligro que deben ser neutralizadas del modo que sea.<sup>382</sup>

Del mismo modo, la IEcG es posible entenderla como una disciplina que busca vislumbrar las debilidades y retos a la defensa y el mantenimiento de las capacidades de producción, el empleo y las políticas de desarrollo de un Estado para garantizar sus posibilidades de supervivencia en el sistema internacional. Precisamente, un área clave de cuidado para la inteligencia

## Gestión de Inteligencia en las Américas

gubernamental como sustento a la política y protección del sistema económico en general, incluiría la comprensión de las intenciones de los competidores económicos internacionales; el análisis de tendencias económicas y negociaciones y la asesoría a los políticos para que entiendan las “reglas del juego económico” (desinformación, regulaciones, dumping, sobornos, cabildeo, boicots, bloqueos, embargos, entre otras) y como son practicadas por los competidores.

### *Situación doctrinal de la IEcG*

Con alguna reserva, son vagos los conocimientos e investigaciones de inteligencia en los países andinos que se enfoquen en las actividades económicas de negocios y financieras compatibles con la inteligencia gubernamental, a excepción de Venezuela<sup>383</sup> y en algún modo Ecuador, país con débiles medidas de inteligencia operativa financiera en prevención y detección oportuna de operaciones contra el lavado de activos y la financiación del terrorismo.<sup>384</sup>

Ciertamente poca es la literatura relacionada sobre el tema y el alcance de la IEcG; no obstante, al examinar la realidad académica española en esta materia, existe un intento por atender esta necesidad, que revela cómo la inteligencia pública se orienta a la obtención de información que aporte luz sobre la afectación a la seguridad nacional por medio de la gestión clandestina y confidencial del recurso humano; en contraste con una inteligencia económica alimentada mayormente de un sistema de observación, monitorización y explotación de fuentes abiertas de información que interactúa con la inteligencia de empresa, a su vez involucrada con una red colaborativa que le entrega *inputs* gubernamentales del extranjero, en algunos casos con información obtenida mediante espionaje de los servicios secretos del Estado.<sup>385</sup>

Así, en la práctica, a pesar de las ágiles reformas económicas implementadas años atrás para la liberación del mercado, expuesto a los obstáculos de rivales internacionales, existe un lento desarrollo de la doctrina en inteligencia estatal en el mundo académico y de seguridad doméstica y regional. De más está decir que para la perspectiva española y esta propuesta, una manera de centrar epistemológicamente la IEcG y la inteligencia económica es abordarlas como combinación de unas disciplinas que surgen a partir de la aplicación convergente de todos los esfuerzos públicos y privados en el ámbito de la sociedad.

*Inteligencia / Economía—Como pueden Acercarse  
los Practicantes*

Una comparación entre la labor e inclinaciones del practicante de inteligencia y el experto en economía y ciencias afines suele verse distante e incluso incompatible, debido a que el ciudadano conoce más la tarea del economista que generalmente trata con datos públicos y tiene un mayor reconocimiento público y social. Cabe consignar que además,

A primera vista, los economistas y analistas de inteligencia parecen operar en separadas esferas, unos tratan con problemas económicos, los otros investigan temas de seguridad. El economista trabaja con gran cantidad de datos, mientras el analista de inteligencia con datos que pueden ser secretos. Las estimaciones del economista son basadas en métodos cuantitativos formales, mientras que el analista de inteligencia a menudo hace sus evaluaciones basadas en la especulación y "sensaciones viscerales e instinto".<sup>386</sup>

No se puede perder de vista que la inteligencia tiene la responsabilidad de producir un conocimiento sobre las posibles intenciones del adversario, basado en datos e informaciones en ocasiones incoherentes y difíciles de adquirir; consecuentemente, la calidad y crédito de la información está sujeta a un proceso que demostrará la capacidad deductiva e inferencial del analista.

Puede decirse que el comportamiento profesional de los economistas reside en el amplio desarrollo teórico de su disciplina académica. Es decir, cualquier economista respalda sus argumentos haciendo referencia a los resultados de los experimentos de políticas públicas (mediante el empleo de datos públicos, producto de políticas económicas que hace algún tiempo entraban en vigor), así contribuyendo con la teoría y la aplicación ética de su perspectiva disciplinar.

Al contrario, el especialista en inteligencia expone un punto de vista menos legítimo por ser menos examinado, dada su escasa experiencia personal y capacidad individual de producir inferencias basadas en datos incoherentes y escasos.

Para el caso colombiano, otro aspecto común a estas dos actividades es no contar con una masa de economistas con un mayor prestigio educativo,<sup>387</sup> de

## Gestión de Inteligencia en las Américas

tecnologías de punta, de conocimiento sistematizado y la resistencia a seguir unos protocolos; situación que alienta una “cultura” del uso de la intuición no óptima para un proceso decisional.

Entonces, a raíz de la inexistencia de una IEcG ¿Puede la presentación de una teoría de inteligencia, asociada a los problemas de competencia económica en el Área Andina, servir para la mejora y la capacidad profesional de un equipo de IEcG?

### Aplicación teórica—la teoría de Sims

En el escenario internacional la influencia de esta clase de responsabilidades, enfrentar contendientes no es nueva y supone que estos no subestiman el concepto de inteligencia, entendida por Sims como el conocimiento útil resultante de la reunión de información, análisis y difusión de la misma a favor de la causa de los decisores, que les brinde decisiones ventajosas respecto de sus rivales.<sup>388</sup> Básicamente la teoría de Sims, se constituye, hasta ahora, como la aproximación más real de apoyo a este propósito investigativo, que identifican cuatro funciones críticas de amplio alcance: reunión, transmisión, anticipación, y manipulación (para influir y deteriorar la capacidad del opositor)<sup>389</sup> y ofrece un medio sistemático y medible del éxito en determinadas actividades, para evaluar un estudio de caso en su aplicación.

### Visión empírica: la IEcG en el proceso decisional en Colombia

#### *Estudio factual 1: seguridad externa*

**Antecedente:** En el contexto geopolítico vivido por el país, la estatal Petróleos de Venezuela - PDVSA mostró interés en comprar la Empresa Colombiana de Gas - Ecogas, la más amplia red para el transporte de gas natural que distribuye el 45% del gas domiciliario en Colombia, y en asociarse con la refinería del puerto de Cartagena. Ésta sería una extensión lógica del ducto para gas y crudo que la empresa planea construir a través de Colombia de manera de transportar combustibles desde Venezuela a Panamá, dijo [el ex presidente de PDVSA Luis] Giusti.<sup>390</sup>

Todo esto preocupó a expertos y dirigentes de Colombia, ante la posibilidad de ceder el control de un sector estratégico a los objetivos políticos más allá de los económicos de Hugo Chávez, en razón a la alta carga ideológica empleada

al momento de hacer uso de su arma estratégica, la diplomacia petrolera,<sup>391</sup> para desarrollar su llamada Revolución Bolivariana y fortalecer su liderazgo en Hispanoamérica. Para aclarar la magnitud del riesgo y amenaza,

En opinión de [Juan Manuel] Santos [ex ministro de la defensa y hoy presidente de Colombia], las intenciones del presidente venezolano, Hugo Chávez, de invertir en el sector de petróleo y gas colombiano pueden ser "peligrosas" debido a que más que un interés económico se percibe una motivación política ... El gas natural beneficia a miles de usuarios colombianos y en caso de algún inconveniente político con Chávez, éste puede simplemente cerrar la "llave" de suministro del combustible y perjudicar a la nación.<sup>392</sup>

A ello se suma el hecho de que PDVSA iba extendiendo sus actividades más allá de la economía insertándose en la política exterior, las relaciones económicas internacionales, la estrategia de alianzas externas y las políticas de defensa de la nación, todas marcadas por el componente anti-imperialista. Se convierte así PDVSA en uno de los instrumentos clave para la ejecución de los lineamientos de seguridad y defensa, junto con la Fuerza Armada.<sup>393</sup>

Por alarmista que parezca lo anterior, esto no es más que una cara del problema, pues en esta frontera tratar el comercio ilícito como mero "contrabando" y a quienes participan en él como a simples "criminales", reduciendo la solución a su aspecto "policial", constituye un error,<sup>394</sup> en razón a que las fronteras crean oportunidades de obtener beneficios para las redes de contrabandistas a la vez que debilitan a los Estados-nación al limitar su capacidad de frenar las embestidas de las redes globales que dañan a sus economías, corrompen a sus policías y socavan sus instituciones.<sup>395</sup>

De este mismo modo, podrá existir un férreo control fronterizo a los bienes, servicios y mano de obra ilícitos que pasan a uno u otro lado de la frontera, pero determinados cargos públicos claves, juzgarán más importante defender el lucrativo comercio ilícito e intereses económicos y políticos de las redes delictivas y así mantener y fomentar el surgimiento de nuevos centros de poder económico criminal.<sup>396</sup>

*Evaluación de inteligencia:* desde el punto de vista defensivo, es de suponer que Chávez haya enfocado la vigilancia en los agentes económicos, los

## Gestión de Inteligencia en las Américas

recursos naturales, el proceso de industrialización de estos y el comercio internacional de Colombia, por lo que el conocimiento por él obtenido sea un arma para una potencial acción bélica, donde la sorpresa estratégica puede pasar de lo económico a lo militar.

Frente a tan sombrío panorama, no puede ser un despropósito considerar las palabras del economista francés Frédéric Bastiat, que encajan en una realidad de frontera donde el comercio ilícito se ha mantenido por años, “cuando a las mercancías no se les permite cruzar las fronteras, los soldados lo harán” o “sí el algodón, el azúcar y el arroz pueden cruzar fronteras, entonces quizás los terroristas no serán capaces de hacerlo”,<sup>397</sup> máximas bien probadas en círculos de planificación estratégica, que encajan con las medidas económica y militar de la vecina nación regentada por un gobernante que ha restringido los negocios con Colombia y robustecido su aparato militar en la línea de frontera, de modo que hace uso de la fuerza disuasiva por medio de las sanciones económicas y su poderío militar para modificar las preferencias de un Estado más débil.<sup>398</sup>

*El proceso de decisión:* en los últimos años han surgido dificultades en las relaciones económicas y comerciales con Venezuela y se percibe que funcionarios de los círculos gubernamentales, consultores privados y fondos de promoción comercial, entre otros, hayan hecho hincapié en las virtudes de probidad y prudencia para reunir información esencial gracias a la socialización con diplomáticos extranjeros y a la evaluación de sus impresiones, en apoyo a empresas de sectores estratégicos en expansión o en dificultades que puedan correr el riesgo de ser adquiridas o intervenidas por el gobierno venezolano.<sup>399</sup>

Al final estos eventos deberían conducir a que agentes gubernamentales y particulares de Colombia, busquen ejercer influencia o defender sofisticadamente la posición de los intereses nacionales en el exterior y acudir a una red de integrantes del servicio de inteligencia gubernamental, encargada de llevar el pulso a los acontecimientos de esta naturaleza, reunir información e identificar con anticipación las acciones políticas con afectación a las inversiones, los capitales y el comercio exterior nacional.

A todas luces, se estaría en presencia de unos actores atados a la definición de la inteligencia del realismo adaptativo, que tiene por objeto explicar el impacto de la información y su gerencia sobre los resultados de la contienda



entre Estados u otros actores en el sistema internacional; es decir, que dirigen la información y explican su impacto para advertir, anticipar y contener los propósitos de la otra parte.

Después de todo, a pesar de la presencia en Colombia de funcionarios y empresarios en posiciones de liderazgo político y económico con poca experiencia en el mundo de la inteligencia, no es extraño resaltar que en los negocios, la política o los deportes, el propósito de la inteligencia es la misma: obtener una mejor información sobre los planes relevantes del oponente, capacidades, normas, y el terreno a menudo por medio del conocimiento secreto.<sup>400</sup>

Cabe insistir en que el imperativo de los funcionarios con poder político será tomar determinaciones y producir resultados con rapidez y confianza, para eso un reto será comprender la importancia y la atención a los asuntos de la IEcG, su función anticipatoria, y la naturaleza de los problemas relacionados con este ámbito de la inteligencia de Estado. En estas condiciones, el poco entendimiento de mecanismos de la inteligencia les conducirá a altos niveles de incertidumbre dentro de la gestión de gobierno debido a la falta de mayor juicio de lo que conocen, de lo que no conocen y de lo que quieren conocer.

## Estudio factual 2: seguridad interna

*Antecedente:* a causa de la perturbación social generada en el año 2008 por un alto número de ciudadanos perjudicados por la confianza puesta en captadores no legales de dinero (pirámides), en algunos departamentos del sur del país (Cauca, Nariño y Putumayo), donde la presencia de cultivos ilícitos y el poder económico del narcotráfico ha sido alta, la administración Uribe declaró el Estado de Emergencia Social, para suspender, intervenir y endurecer las penas contra esta clase de prácticas. Esta decisión centró su interés en recuperar y reintegrar los dineros para mejorar el clima de negocios en las regiones afectadas.

Compatriotas. El delito de captación masiva e ilegal de dinero, cualquiera sea la modalidad, cualquiera sea la ficción detrás de la cual se esconda, cualquiera sea la carta de presentación, es un delito contra el orden económico y social, genera profundas perturbaciones sociales [...] Y generalmente se combinan esos faltantes de dinero con robos del dinero, porque

## Gestión de Inteligencia en las Américas

estas entidades no tienen vigilancia de instituciones oficiales, además no cumplen los requisitos de la ley y todo termina en una grave perturbación social.<sup>401</sup>

A su vez, se han dado a conocer los presuntos nexos entre la captadora ilegal y uno de los frentes de las FARC (Fuerzas Armadas Revolucionarias de Colombia), así como las desavenencias surgidas con la cúpula de esta organización obedecidas al manejo financiero de uno de sus frentes.

Aunque a cuenta gotas, las autoridades han venido revelando por estos días el contenido de lo que al parecer es el computador de alias "Édgar Tovar", jefe del frente 48 de las Farc que delinque en Putumayo. Como se sabe, David Murcia Guzmán, el cerebro del [Grupo holding] DMG, tenía su epicentro en Puerto Asís y fue desde allí que comenzó a expandir su negocio. [ ... ] Dice la Policía que el computador, hallado durante la Operación Fortaleza realizada el pasado 20 de enero, guardaba la lista de sanciones del secretariado de las Farc a este grupo por haber invertido 15 mil dólares (unos 30 millones de pesos) en DMG, sin autorización de lo que ellos llaman Estado Mayor.<sup>402</sup>

*Evaluación de inteligencia:* quedó claro que la práctica ilegal de estos “empresarios”, colocó en riesgo la seguridad del Estado, ya que se hizo evidente la alta tasa de afectados, que condujo al incremento de la inseguridad e inconformismo que habría sido capitalizado por el terrorismo.

El gobernador de Putumayo, Felipe Guzmán, denunció ante el Presidente Álvaro Uribe que las Farc estarían aprovechando del descontento de la gente por el tema de las pirámides para poner al pueblo contra el gobierno. El funcionario aseguró que desde el pasado domingo las Farc han utilizado explosivos, han amedrentado a los campesinos y han difundido panfletos para influenciar a los habitantes de las regiones más afectadas por el tema de las pirámides.<sup>403</sup>

Más allá de la afectación a la seguridad, Eduardo Sarmiento, decano de la Facultad de Economía de la Escuela Colombiana de Ingeniería, informó a la

prensa que el gobierno “se enredó” en una discusión semántica de si eran o no pirámides, “cuando lo que debieron hacer fue evaluar sus balances y declaraciones de renta y allí se hubieran dado cuenta de que los pasivos superaban el activo y había un riesgo”.<sup>404</sup>

*El proceso de decisión:* el gobierno de ese entonces no obtuvo un conocimiento claro de la situación como resultado de esos posibles datos, información, evidencias y evaluaciones de inteligencia, presentados sin un apropiado contexto debido a la naturaleza especializada de la información. Declaró el ex ministro de Hacienda Juan Camilo Restrepo, “Creo que hubo tardanza injustificada por parte del Gobierno en tomar medidas preventivas. El problema de las pirámides venía advirtiéndose hace más de un año, o año y medio”.<sup>405</sup>

No es ligero, ni arbitrario, pensar que este hecho dejó entrever la ausencia de una IEcG que se adelantara a situaciones de esa naturaleza y alertara a los centros de poder de decisión, para evitar la tardía reacción gubernamental a pesar de las advertencias.

### Una doctrina aplicada a la IEcG: las funciones críticas del realismo adaptativo

Conocido es que las amenazas a las economías nacionales parecen de imposible eliminación; no obstante, aplicar preventivamente acciones de inteligencia y contrainteligencia a potenciales conductas punibles contra el orden en los sectores y actividades económicas prioritarias, conduciría a mejores consideraciones para atenuarlas. Efectivamente, una obtención del insumo informativo contribuirá a que el gobierno adopte decisiones administrativas o de carácter penal, para combatir las acciones desestabilizadoras y delincuenciales que se mueven entre la esfera legal e ilegal. En esta parte del ensayo, se muestran las condiciones para ofrecer un esquema que daría luz a una IEcG operacional.

Al concebir la IEcG como una actividad en el ámbito económico externo, como sería de aplicación al primer estudio del caso, la incorporación de un programa de inteligencia y contrainteligencia económica tendría que medir el efecto en las relaciones con los países andinos, iniciativa que podría socavar la confianza y paralizar los esfuerzos diplomáticos con naciones en las que tradicionalmente existe una mutua dependencia económica y que actualmente son

## Gestión de Inteligencia en las Américas

propensas a tener diferencias políticas y ser hostiles con los actores afectados por estas.

Desde esta base de entendimiento, a continuación se enseña la implementación sistemática de cuatro funciones críticas para una IEcG en los sectores económico, financiero y de comercio internacional, pues la atención de la inteligencia y la contrainteligencia no podrían cubrir todo el espectro económico, observación que conduciría a un objetivo poco realista en razón a su magnitud y diversidad.

Por supuesto, la información que relacione a todos los países andinos no está disponible debido a la naturaleza secreta de la misma. Bajo esta condición limitante de información incompleta, se experimenta una realidad que desafía la tarea de los profesionales de inteligencia e ilustra mayormente la teoría de Sims.

### *Reunión de información*

En términos que reflejan la visión de Sims, esta función debe contar con fuentes de inteligencia abierta y humana para apoyo de la IEcG; en legaciones diplomáticas, representaciones comerciales y empresas públicas y privadas, y el empleo de seleccionados, confiables y avezados agentes de inteligencia que adquieran clandestinamente -por espionaje- la información económica, comercial y financiera mediante el uso de métodos y fuentes de inteligencia. A su vez, la participación de un equipo de inteligencia dará una oportunidad laboral para economistas y otras profesiones afines, que familiarizados con la actividad y habilidades en inteligencia, conozcan información de primera mano sobre las instituciones y los agentes con poder e influencia económica en el exterior y accedan a su círculo interno para así obtener, procesar y difundir información sobre los blancos de interés. Como sostiene un informe de la revista *Semana*,

La mayoría de los agentes secretos son hombres callados y muy discretos, capaces de infiltrar sin mayor sospecha altos círculos diplomáticos, gubernamentales o empresariales. Mimetizados en perfiles que van desde estudiantes de intercambio, empresarios, turistas y trabajadores de una multinacional, la gran mayoría difícilmente utilizaría un arma para conseguir sus objetivos. Por el contrario, uno de

## Russell G. Swenson y Carolina Sancho Hirane

ellos le dijo a SEMANA que su misión se asimila más a la de un procesador de datos que se dedica a recopilar información valiosa, procesarla y entregarla a su gobierno.<sup>406</sup>

Consecuentemente con la inteligencia humana o reunión de información con injerencia en el plano económico, según revelaciones de *El Espectador*:

*El condenado ex director de Inteligencia Fernando Tabares aportó nuevos detalles a la Corte. Relató que la Embajada de Venezuela en Colombia acreditó a 80 funcionarios que hacían inteligencia para el gobierno Chávez, que el DAS encontró órdenes de operaciones de la Dirección de Inteligencia de ese país (Disip) en ese sentido y se destapó que algunos estamentos económicos, militares y hasta políticos del país fueron “penetrados”.<sup>407</sup>*



**Figura 6.** Uff. Que riesgosa tarea la de hoy. Esta información bastará para mañana.

**Fuente:** Cortesía Andrés González (GOVA).

Desde un punto de vista de contrainteligencia, estas evidencias, permiten considerar que la IECG colombiana esté centrada en la reunión de noticias y

## Gestión de Inteligencia en las Américas

reportes de las condiciones económicas en áreas vitales para la seguridad nacional, a la vez que es guiada por las observaciones efectuadas a la inteligencia venezolana favorecida con un amplio rango de operaciones, debido al poder financiero sustentado por la actividad petrolera que le permite mayor acción y movilidad frente a sus rivales.

### *Anticipación*

Dos capacidades esenciales constituyen esta función. Una relacionada con la habilidad de reunir información independientemente de las preferencias habituales o la aprobación de los responsables políticos y la otra con la habilidad de crear la necesidad de proveer advertencias inesperadas y la identificación de nuevos competidores o adversarios.<sup>408</sup>

Luego habrá de considerarse el estímulo a la iniciativa individual de competentes expertos que asuman riesgos a hacer algo más allá de lo estipulado, así fuere inconsistente con la visión de los decisores mas no de los objetivos de éstos, para conocer y advertir quiénes son los nuevos adversarios y el alcance de su poder en el mundo de las relaciones económicas, de negocios y financieras internacionales, así como la capacidad de proteger las fuentes y los métodos para reducir las vulnerabilidades. Así se explica que la IECG debe prever los desafíos y oportunidades a los que generalmente los responsables políticos dan poca atención, y alertar a esos a quienes pueden ser excluidos de los círculos más cercanos a la formulación de la política económica pública.

Evidentemente, algunos de los problemas económicos son el resultado de acciones políticas de países extranjeros y en otras circunstancias, a desatinadas declaraciones de influyentes actores domésticos. De este modo, Colombia no fue capaz de anticipar la crisis comercial con Venezuela debido, entre otras medidas, al control de cambios que alegó Venezuela por razones de interés nacional y que ha tenido al borde de la quiebra a los exportadores colombianos por la demora en la entrega de divisas para pagarles.<sup>409</sup> De igual manera, las declaraciones de los dirigentes gremiales de Analdex (Asociación Nacional de Exportadores) y Andi (Asociación nacional de Industriales) sobre el golpe de Estado que sacó temporalmente del poder a Chávez (abril 2002) y que generó el veto a algunas empresas colombianas instaladas en el vecino país.<sup>410</sup>

Como en los casos anteriores, a raíz de la Operación Fénix (marzo 2008) en la que el Ejército de Colombia abatiera a “Raúl Reyes”, cabecilla de las Farc, en territorio ecuatoriano, que llevaron al deterioro de las relaciones entre Ecuador y Colombia, el gobierno de Rafael Correa decidió imponer una salvaguardia cambiaria (julio 2009) a Colombia por su política monetaria,<sup>411</sup> por lo que la consabida afectación al intercambio comercial comenzó a manejarse en el terreno político.

En este sentido, se develó la ausencia de emisarios que bajo el refinado y discreto empleo de fuentes humanas, obtuvieran información privilegiada para anticipar estos acontecimientos y mitigar riesgos políticos con implicaciones para la seguridad y los intereses económicos de Colombia en Venezuela y Ecuador.

Por consiguiente, la aplicación de estas capacidades para anticipar nuevos riesgos puede verse entorpecida por la resistencia de los decisores a los cambios de la agenda, la atención a múltiples actores en contienda, el rechazo a nueva información que no sea consistente con sus prioridades, la parroquial visión del mundo, objetivos distintos a los económicos que revistan mayor importancia en lo coyuntural y en el peor de los casos posibles intereses creados.

### *Transmisión*

Identificado el adversario y su poder habrá de conocerse a quien transmitir esa información, función que requerirá la confianza entre el proveedor de inteligencia y el decisor, confianza, que podría estimarse de acuerdo a la proximidad del servicio de inteligencia con el decisor y fundamentada en la prioritaria entrega de información con un alto alcance y utilidad para la toma de decisiones.

Una precisión adicional hace referencia a que cuando la inteligencia concibe su misión como independiente y aislada del decisor, surgirá una fractura que puede ser una fuente de rivalidad por el poder, por lo que la transmisión de la inteligencia decaerá o fracasará; sin embargo, una excesiva proximidad al decisor también es inconveniente si conduce a la incapacidad para anticipar sus errores. De ahí que el Presidente Chávez hizo uso de dos servicios de inteligencia (nacional y extranjera), para ampliar su visión y escucha al informarse de manera oportuna y con tiempo para actuar y evitar errores, y con la intención



**Figura 7.** Urrg....;¿Estás diciendo la verdad, toda la verdad y nada más que la verdad?!

**Fuente:** Cortesía Andrés González (GOVA).

La injerencia cubana en Venezuela “tiene escandalizados hasta a los propios chavistas” <sup>412</sup>. Relata Américo Martín, ex guerrillero y político venezolano estudioso del tema cubano,

En este momento se multiplican en el ámbito militar y de inteligencia y contrainteligencia. Hay una densa penetración ideológica. Miembros de milicias, militares profesionales y centenares de dirigentes se están formando en Cuba -asegura Martín-. Chávez percibe como enemigos a los disidentes y en la medida en que retrocede, denuncia magnicidios y golpes. No confía en sus seguidores, exige lealtad absoluta, y sólo se siente seguro rodeado de enviados de Fidel.<sup>413</sup>

De manera similar puede considerarse que el decisor reúna su propio conocimiento en inteligencia, mediante la transmisión de información de individuos particulares alejados de la opinión pública y en posiciones de poder; empero,



él deseará extender sus ojos y oídos mediante un servicio de inteligencia que evalúe los datos recogidos en su nombre y con la creación de mecanismos de rendición de cuentas y vigilancia que garanticen la lealtad a su causa y política. Esta perspectiva se comenta de modo irónico en un periódico caraqueño:

Cuando digo un pueblo sin memoria, me refiero a que los venezolanos olvidan el acuerdo bilateral con La Habana que permite a personal policial y de seguridad estatal cubano realizar en Venezuela tareas de espionaje y policiales. Cuando digo un pueblo malagradecido, me refiero a la ingratitud de los venezolanos por el control del Departamento de Seguridad de Cuba (G2) de los servicios de inteligencia, de identificación e inmigración, y los registros públicos y notarías; vigilando con ello al ciudadano, su identidad, documentos personales y propiedades.<sup>414</sup>

Esta opinión periodística evidencia que la visión de seguridad de un líder político (Chávez y su apoyo a la injerencia cubana en asuntos de seguridad) no siempre es compartida por todos los venezolanos. Además, en términos de transmisión de perspectivas de inteligencia a la máxima autoridad, sería claro que el valor de un hombre de confianza puede medirse si genera una alerta o no a su mandatario sobre los ingeniosos puntos de vista ocultos de los adversarios.

### *Contrainteligencia*

En un mundo globalizado y competitivo como el que rige las relaciones económicas y comerciales entre los Estados, existe la tendencia a vulnerar la ley mediante el espionaje. Es por ello por lo que la razón para la aplicación de medidas de contrainteligencia, obedezca a la necesidad de contrarrestar la acción del oponente que menoscaba la eficiencia misional de una forma u otra del servicio. Por tanto, la existencia de la primera se debe a la segunda.

Dice el realismo adaptativo que en un conflicto de intereses hay dos maneras de tomar una decisión ventajosa. Bien mediante la reunión de la mejor información sobre las actividades del adversario, o distorsionando la información del oponente mientras protege la propia (contrainteligencia); esta última cuenta con dos componentes, defensivo y ofensivo.

Tabla 9  
Dos Componentes de Contrainteligencia

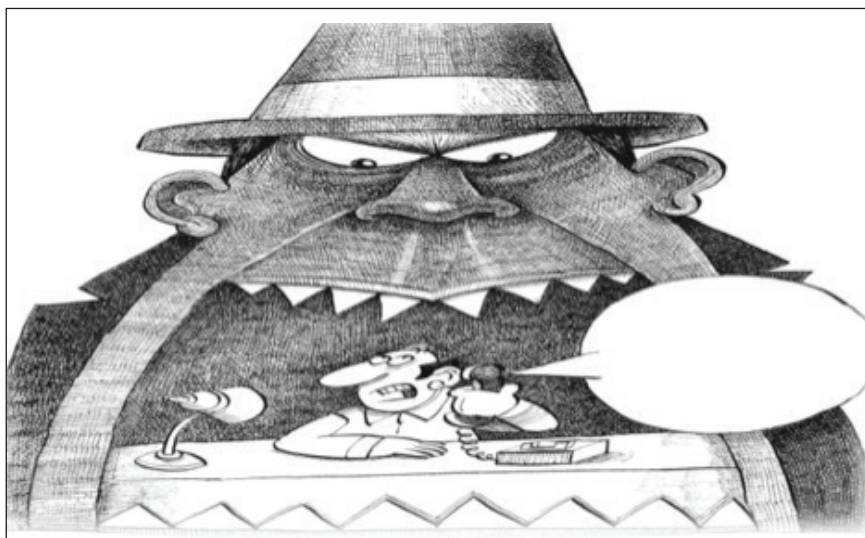
<b>CONTRAINTELIGENCIA</b>	<b>Defensivo:</b> La protección informativa del servicio mediante el bloqueo a la recolección de información de otro servicio.
	<b>Forma pasiva</b> (preventiva): Incluye el empleo de: vigilantes, bóvedas de seguridad, desertores, interrogatorios, espías y similares.
	<b>Forma activa</b> (operativa): Involucra el seguimiento a espías, o la provocación y burla al servicio hostil al tomar parte en la revelación de sus métodos por medio de señuelos para distraer su atención. Con esto se busca evidenciar una plena acción de actividad hostil de individuos u organizaciones sospechosas.
	<b>Ofensivo:</b> No es bloquear las operaciones del oponente. Es cambiar o romper las intenciones del adversario al jugar con su mente. Su propósito es defender las propias operaciones para desviar la información del oponente. Obtener ventajas para sí mismo mediante el uso de mecanismos que permitan la manipulación o el sesgo de las capacidades de inteligencia de los demás, para con ello impactar su actividad de inteligencia y perspectiva de supervivencia.
<b>CONTRAINTELIGENCIA</b>	<b>Forma pasiva</b> (preventiva): Involucra prácticas ficticias o camuflaje. Fachadas de personas con disímiles trabajos o personas con interés en establecer por medio de la empatía una “amistad” u otra intensión, que tenga como fin oculto el obtener información sensible.
	<b>Forma activa</b> (operativa): Involucra el uso de agentes dobles y el engaño. Es decir el responsable ayuda al engaño para conducir al adversario a falsos juicios mediante el reclutamiento de agentes dobles con habilidades musicales, coreográficas, etc. La acción de desinformación se basa en ocultar las actividades, los intereses informativos específicos e intenciones del servicio de inteligencia, y el desvío de la atención de quienes realizan el espionaje hacia otros objetivos de menor valor.

**Fuente:** Creado por el autor.

Un ejemplo notorio que involucra al gobierno venezolano con asuntos de inteligencia y economía, se da a conocer con el siguiente señalamiento a un funcionario de inteligencia militar:

José Gregorio ‘Cheo’ Guzmán llegó a Colombia en 2003 como oficial de la embajada de Venezuela, con el supuesto encargo de facilitar negocios entre empresarios de ambos países. Aunque su cargo no era de primera línea, en poco tiempo empresarios y políticos se dieron cuenta de que éste era el hombre de Chávez en Bogotá. Reconocido militante del partido Patria para Todos, se le conoce por ser muy cercano al Palacio de Miraflores, a pesar de que mantiene un bajo perfil.<sup>415</sup>

Conforme con este episodio que saca a la luz la función de contrainteligencia colombiana defensiva-activa porque “en poco tiempo empresarios y políticos se dieron cuenta de que éste era el hombre de Chávez en Bogotá” y que tal vez abarcó actividades como el seguimiento a este individuo, entre otras, característica ajustada a la descripción de la tabla anterior.



**Figura 8.** ¡Jefe. Creo que esta vez habrá novedades!  
**Fuente:** Cortesía Andrés González (GOVA).

## Gestión de Inteligencia en las Américas

A esto hay que adicionar otro antecedente sobre la irregular manipulación económica en favor de la política expansionista chavista en el país, develada en las presiones de los enviados del gobierno bolivariano de Venezuela, con órdenes explícitas para usar recursos privados de la empresa [Monómeros Colombo Venezolanos] en la financiación de personas y entidades cercanas al movimiento bolivariano en Colombia.<sup>416</sup>

Pasando a la literatura militar y en el ámbito del orden público interno, otra reseña que ilustra la misma función con la aplicación del componente ofensivo en su forma activa y pasiva, son las importantes vivencias de un suboficial del Ejército de Colombia en la década de los 60; que gracias a las operaciones encubiertas y la aplicación de fachadas, el engaño, la manipulación y otros mecanismos influyeron en la voluntad, la información y las acciones de los bandoleros rurales que en ese entonces, como en la actualidad, robustecían sus finanzas mediante la extorsión, la exigencia de “impuestos” y otras acciones criminales acompañadas del apoyo de acaudalados propietarios o de políticos de alguna significación en las provincias.<sup>417</sup>

### En resumen

Así en la práctica y frente a las evidencias anteriores, se espera que una herramienta clave para considerar la aplicación real de estas funciones en la IEcG, sea el reconocimiento del ciclo de inteligencia como una labor pública, así el proyecto de ley estatutaria 195, en su artículo 4 literal c, señala que la información de inteligencia y contrainteligencia podrá ser obtenida con el fin de proteger los recursos naturales y los intereses económicos de la nación, asunto que reconoce la injerencia de los organismos de inteligencia en resguardar la inversión, el comercio, el desarrollo económico y por tanto la seguridad económica nacional.<sup>418</sup>

En síntesis, los puntos anteriores revelan en su totalidad una aplicación sistemática de los principios de IEcG, por parte de los servicios secretos y otros actores atentos a fenómenos económicos que generan problemas a la seguridad nacional. Seguidamente, aparece un cuadro que esquematiza los puntos a tener en cuenta a la hora de reconocer una importante y cuidadosa gestión de los servicios de inteligencia y otras entidades económicas gubernamentales, que con su colaboración profesional puedan fortalecer la comunidad de inteligencia.

Tabla 10 Pautas para Acción Colaborativa por un Equipo de Inteligencia Económica Estratégica		
Funciones Sims	Actividad	Entidades
<b>Reunión de Información</b>	<p>Identificar los actores económicos claves, su reputación y sus capacidades. (Situación financiera, planes de desarrollo y relaciones económicas y comerciales con el exterior).</p> <p>Acordar el desarrollo de apreciaciones, análisis y aportes investigativos con académicos y consultores públicos y privados del ámbito económico.</p> <p>Reunir información relacionada con la intromisión de grupos armados ilegales y agentes corruptores en asuntos económicos.</p> <p>Monitorear la economía nacional e internacional en la Web y suscripciones especializadas.</p> <p>Planificar y apoyar objetivos de política exterior.</p>	<p>Planeación Nacional.</p> <p>Hacienda y Crédito Público (Unidad de Información y Análisis Financiero - UIAF y la Dirección de Impuestos y Aduanas Nacionales - DIAN).</p> <p>Ministerio de Comercio, Industria y Turismo.</p> <p>Ministerio de Relaciones Exteriores.</p> <p>Ministerio de Minas y Energía.</p> <p>Gremios económicos - Consejo Gremial Nacional y Cámaras de Comercio.</p>
<b>Anticipación</b>	<p>Prever los intercambios ilegales en mercados negros y oportunidades que favorezcan la corrupción.</p> <p>Acudir a agentes experimentados que valoren los riesgos a intereses económicos nacionales en el exterior.</p>	<p>Planeación Nacional.</p> <p>Hacienda y Crédito Público (Unidad de Información y Análisis Financiero – UIAF y la Dirección de impuestos y Aduanas Nacionales -DIAN).</p> <p>Ministerio de Relaciones Exteriores.</p>

## Gestión de Inteligencia en las Américas

Tabla 10, (continua) Pautas para Acción Colaborativa por un Equipo de Inteligencia Económica Estratégica		
Funciones Sims	Actividad	Entidades
<b>Transmisión</b>	Divulgar evaluaciones de riesgo y advertencias frente a amenazas de naturaleza económica, de negocios y finanzas internacionales.	Planeación Nacional.  Gremios económicos – Consejo Gremial Nacional y Cámaras de Comercio.
<b>Contrainteligencia</b>	Neutralizar operaciones de inteligencia de actores hostiles que amenacen los activos e infraestructura estratégica y seguridad económica nacional.  Vigilar zonas urbanas y rurales con proyectos en desarrollo de alto impacto ambiental y valorización de tierras.  Operar en áreas donde no hay información abierta y en las que el sector privado no pueda acceder.  Atender requerimientos informativos especiales.	Hacienda y Crédito Público (Unidad de Información y Análisis Financiero – UIAF y Dirección de Impuestos y Aduanas Nacionales – DIAN).  Ministerio de Comercio, Industria y Turismo.  Ministerio de Agricultura.

Fuente: Creado por el autor.

### Un acercamiento a la IEcG a nivel estratégico dentro de la comunidad de inteligencia

La seguridad nacional orientada al cumplimiento de unos objetivos nacionales, resalta el desarrollo económico. En ese orden de ideas, en el marco del interés nacional, la incipiente IEcG se ha encaminado prioritariamente en obtener información para desmontar la estructuras de apoyo de actores armados por fuera de la ley, y a prevenir atentados contra la infraestructura económica crítica del país; es decir, se sabe actuar a nivel operacional dada la vasta actividad terrorista en esos blancos.

Ahora bien a escala estratégica, el terrorismo en Colombia combina todas las formas de lucha y emplea la guerra económica tangible al dañar la infraestructura económica estratégica (represas, oleoductos, vías, aeropuertos, sistema de transmisión eléctrica, etc.), por lo que ha obligado a la cooperación entre gobiernos e inversionistas para proteger sus intereses en ambas vías.<sup>419</sup>

Pasando a otro plano, Colombia cuenta con una institución de inteligencia financiera de carácter estratégico. El establecimiento en 1995 del Grupo Egmont que reúne las Unidades de Inteligencia Financiera del mundo incluyó la Unidad de Información y Análisis Financiero de Colombia -UIAF- para intercambiar información con las demás UIF del mundo, lo que facilita luchar contra delitos de lavado de activos y financiación del terrorismo.<sup>420</sup>

La UIAF como parte de la comunidad de inteligencia del país, cumple una función a nivel de inteligencia y contrainteligencia operacional, dentro de un andamiaje estratégico internacional. Su misión es prevenir y detectar operaciones relacionadas con el lavado de activos y la financiación del terrorismo, mediante la centralización, sistematización y análisis de información con el fin de entregarla a las autoridades competentes. Por lo visto en su gestión, el perfil profesional para el cumplimiento de su misión muestra homogeneidad entre la formación y el nivel académico de los funcionarios de la UIAF, el 77,6% de los funcionarios son profesionales, el 54,7% han realizado un estudio avanzado a nivel de especialización o maestría.<sup>421</sup>

Es por ello que la IECG inserta en una sociedad de la información, debería contar con alianzas estratégicas con el mundo privado, de similar naturaleza a las tareas de reporte efectuadas por la UIAF, información para hacer vigilancia y seguimiento a actividades sospechosas, como una respuesta inevitable al sano crecimiento del Estado y la economía, en lugar de ser vista en el imaginario colectivo como una práctica conspiradora.

En lo que respecta a hablar sobre la problemática del comercio ilícito en Colombia, a lo largo de la historia este ha sido una constante, por lo que corresponde considerar que en la Ley de Inteligencia se contemple en la comunidad de inteligencia<sup>422</sup> la incorporación de la Dirección de Impuestos y Aduanas Nacionales (DIAN) para intercambiar información con la Oficina Internacional de Enlace e Inteligencia (RILO), red mundial de aduanas de

## Gestión de Inteligencia en las Américas

todo el mundo, que maneja datos relacionados con las actividades ilícitas en materia aduanera.

Por otra parte, el documento Conpes (Consejo Nacional de Política Económica y Social),<sup>423</sup> inserto en el Plan Nacional de Desarrollo “Estado Comunitario: Desarrollo para Todos 2006–2010”, en concordancia con lo estipulado en la Carta Política,<sup>424</sup> contempló un proceso de fortalecimiento de la inteligencia y la contrainteligencia estatal, para afianzar los logros que venían produciéndose en materia de seguridad; sin embargo, a nivel de la inteligencia civil el proceso no se dio en razón a los frustrados intentos por renovarla y las persistentes malas prácticas internas, que desataron una gravísima falla en la seguridad conocida por la opinión pública nacional e internacional, situación que la han conducido a un cambio de diseño con dedicación exclusiva a las labores de inteligencia y contrainteligencia de Estado como esfuerzo hacia una visión de futuro.<sup>425</sup>

De hecho es admisible pensar en una desconexión disciplinar entre la economía y la inteligencia, que impide al servicio interpretar con antelación y exactitud una multiplicidad de fenómenos económicos con impacto en la seguridad nacional, y que demanda la creación de una unidad especializada que articule con la comunidad de inteligencia,<sup>426</sup> y difunda programas en análisis e inteligencia para comprensión y los límites de estas en los analistas económicos, de negocios y financieros, especializados en el cotejo y análisis sistemático de información en las actividades del mundo oscuro del comercio legal e ilegal que incluyan las redes utilizadas por el terrorismo,<sup>427</sup> la delincuencia organizada y la corrupción en los sectores público y privado.

Así las cosas, el hecho de que la IEcG llegue a ser de miramiento y de apoyo a la acción gubernamental y las relaciones internacionales, supone considerar que la asociación y el uso de un conocimiento compatible entre economistas y analistas de inteligencia, sea una condición que fortalezca las decisiones de gobierno y por qué no para la elaboración de políticas públicas.

### Una estrategia a contemplar para ampliar la visión de la inteligencia nacional

Es deber del Estado proteger la vida y bienes de sus ciudadanos, por eso una acción en defensa de estas en el lugar y momento indicado, previa evaluación del alcance exacto de amenazas percibidas como reales e inminentes, podría



ser válida, si previene un acto que implique una grave afectación de los intereses económicos nacionales; sin embargo, el Estado debe hallar un equilibrio entre las garantías a la seguridad con el respeto a las libertades civiles y los derechos humanos.

En fin, una amenaza de primer orden tal como la guerra económica tangible terrorista desafía la existencia de la nación al haber un ganador y un perdedor (juego de suma cero), aunque un observador de cambios estratégicos sugiere que la geo-economía ha reemplazado a la guerra [tradicional]: “todo el mundo, al parecer, está de acuerdo en que los métodos de comercio están desplazando a los métodos militares - con el capital disponible en lugar del poder de fuego, la innovación civil en lugar de progreso militar - técnico y la penetración del mercado en lugar de cuarteles y bases”.<sup>428</sup>

De tal modo, se entra a una nueva apreciación del hecho que la guerra económica es amplia y continua, y va más allá de los *targets* tangibles. Entonces, para que el esquema institucional actual esté preparado para prevenir y atender esta clase de desafíos cabe preguntar ¿Cómo podrá ajustarse la IEcG a este nuevo paradigma?.

Para ello, sería fundamental tomar en cuenta el sano interés y las opiniones de actores diferentes al Estado sobre la actividad de inteligencia, pues como señala Nicolás Urrutia, investigador de la Fundación Ideas para la Paz, en medio de los escándalos del DAS, se ha pasado por alto que a pesar de las recriminaciones que enlodan el debate, tanto gobierno como oposición coinciden en una realidad de a puño: “Colombia necesita espías.[...] Y en esto coinciden unos y otros las decisiones vitales del Estado deben estar mejor informadas, y el proceso de obtener información necesariamente pasa por el espionaje”.<sup>429</sup>

En vista del problema planteado, es decir, conocer el alcance y la doctrina de un equipo de trabajo oficial para contribuir al logro de los objetivos estratégicos de la inteligencia de Estado, conviene señalar algunas actividades útiles para entender, implementar y obtener resultados deseados de una IEcG capaz de superar los retos en los dos estudios de seguridad externa e interna, arriba mencionados.

Parece válida la opción de incluir una integrada y colaboradora red de trabajo, desde la que los agentes del Estado y la sociedad civil (gremios económicos, academia, etc.) sean parte del diseño, la formulación, la retroalimentación y la inspección de ideas que guarden relación con el desarrollo de cada una

## Gestión de Inteligencia en las Américas

de las funciones de Sims, desafío de una IEcG vinculante y apta para lograr una alianza con todos estos actores, pero la iniciativa para la construcción de alianzas parecería más compleja de lo que parece, como consecuencia de la relación entre el gobierno y los actores sociales, en razón a lo afirmado por la investigadora de la Universidad Externado de Colombia, Marta Ardila:

Tanto el sector empresarial como el académico resultan relevantes en el proceso de toma de decisiones. El primero incide de manera individual por medio de empresarios de sectores específicos o de representantes de conglomerados nacionales y también de manera organizada a través de gremios o de las Cámaras de Comercio. El poder económico de estos sectores permite presionar ciertas decisiones y políticas, tanto en el plano nacional como en el internacional, aunque su participación depende de una coyuntura política. En cambio el sector académico es más disperso y tiende a desconfiar de las acciones gubernamentales. Se considera que muchos de los planteamientos del establecimiento se quedan en el nivel retórico, sin un acercamiento real hacia los actores no gubernamentales.<sup>430</sup>

Por lo visto, la creación de un sistema de IEcG genera reservas en los actores no gubernamentales, que de superar y potenciar las sinergias informativas y conocimiento entre el Estado y la sociedad civil colombiana, podría ser un arma competitiva económica como elemento fundamental de la seguridad.

Ahora, más allá de las técnicas de vigilancia reactivas u otras acciones tácticas, hay que agregar a la IEcG una agenda de actuación pública a nivel estratégico, previa valoración jurídica, que justifique la posibilidad de reunir y difundir información para generar advertencias económicas en los círculos económicos y en entidades públicas, entre otros, para que la inteligencia y el mundo económico público y privado local se movilicen frente a las variadas amenazas y desafíos generados por actores opuestos a los fines del Estado.

Pero para poder progresar en esa dirección, no deja también de ser importante establecer que parte de la atención de la inteligencia gubernamental se deba orientar al mundo económico externo, y evitar que los especialistas se involucren en actividades indebidas asociadas con el ambiente político

interno, para que estén por fuera de una multiplicidad de intereses en pugna y conexiones deshonrosas “locales” y así desarrollar un alto nivel de profesionalismo.

### Biografía del autor

**Álvaro Venegas González**, colombiano, egresado de la Facultad de Ciencias Económicas y Sociales de la Universidad de La Salle en Bogotá y ex servidor público del extinto Departamento Administrativo de Seguridad - DAS. Actualmente promueve la Cultura Nacional de Inteligencia, gracias al tratamiento de temas relacionados con la inteligencia estratégica y seguridad nacional. Ha sido colaborador de las revistas *Aquimindia*, *AAinteligencia* de Chile y *Nova et Vetera* - ESAP de Colombia. Contacto: aljovego@hotmail.com.

### Gestión de Recursos para la Inteligencia

Dan Elkins

Otros autores aquí han notado el rol evolutivo de los poderes legislativos nacionales sobre el control o vigilancia a las agencias de inteligencia. La capacidad del legislativo para llevar a cabo una vigilancia adecuada recae en la habilidad del personal asesor, así como de oficiales designados, para entender el panorama general de los programas de inteligencia, y cómo cada agencia del sistema nacional de inteligencia puede contribuir al logro de los objetivos programados. Especialistas en la gestión de recursos de cada agencia tienen la obligación de mantener un diálogo con expertos del tema en sus agencias, con el fin de preparar planes y presupuestos financieros que serán revisados por oficiales gubernamentales de finanzas, de la rama ejecutiva o legislativa. De hecho, especialistas en la gestión de recursos y funcionarios de inteligencia pueden obtener verdaderos beneficios mediante la interacción con colegas, no sólo de su organismo, sino también con sus homólogos de toda la comunidad de inteligencia; del mismo modo, los expertos en el tema se benefician con el intercambio que suele ocurrir diariamente con sus colegas mientras ellos persiguen objetivos de inteligencia y planes de operación.

El autor de este ensayo está bien familiarizado con la gestión de recursos y los procesos presupuestales de la Comunidad de Inteligencia de los Estados Unidos, es más, los principios y las prácticas que él ha observado y ha experimentado son aplicables también en cualquier otro país, en donde se espera que las agencias de inteligencia rindan cuentas a los ciudadanos que protegen, y a las oficinas gubernamentales designadas para supervisar y proveer los recursos necesarios a éstas para desarrollar sus respectivas misiones.

Los principios y las prácticas descritas en este ensayo son, pues, aplicables a todos los niveles de responsabilidad, como se identificaron en el ensayo de Gonçalves: 1) agencia—interno, dentro de una agencia de inteligencia en particular; 2) ejecutiva—realizado dentro de la rama ejecutiva por entidades de la administración alejadas de la inteligencia y por el departamento o ministerio a la que la agencia de inteligencia está subordinada; 3) externo—ejercido por la rama judicial, por la rama legislativa, y/o por una entidad independiente; y 4) popular—donde se abordan los intereses de los ciudadanos u organizaciones de la sociedad civil. De interés especial aquí son las prácticas

que permiten a los especialistas de gestión de recursos y a los reconocidos profesionales de inteligencia, llevar a cabo la rendición de cuentas al manejo interno de los recursos de las agencias de inteligencia.

Hay tres clases de profesionales que pueden beneficiarse de la lectura de este ensayo. El primer grupo está conformado por profesionales en las prácticas y procesos de gestión de recursos que se explicará más adelante. En el segundo grupo están los profesionales “funcionales,” quienes dirigen y conducen las misiones de inteligencia y actividades conexas (reunión de información, análisis, producción, seguridad, entrenamiento de inteligencia, administración de la información, etc.). La financiación de las propuestas elaboradas por los profesionales de recursos es generalmente dirigida a satisfacer las necesidades que han sido identificadas por los profesionales funcionales. Finalmente, los supervisores de inteligencia, que tienen amplias responsabilidades de gestión de los recursos, necesitan estar familiarizados con los principios que guían el trabajo de los especialistas en recursos para asegurar que esos principios son aplicados.

### El uso eficaz y eficiente de recursos

El éxito en los esfuerzos de una organización para asegurar suficientes recursos, bien puede depender de su trayectoria en el uso eficaz y eficiente de esos recursos adquiridos a través de los esfuerzos anteriores. Uno de los roles principales de una oficina de gestión de recursos es determinar las necesidades de recursos de la organización y tomar la iniciativa en los esfuerzos por satisfacer esas necesidades. Sin embargo, la responsabilidad para asegurar el uso eficaz y eficiente de los recursos existentes descansa en todos los miembros de la organización. Esto incluye a los líderes que establecen las políticas, los gerentes de rango medio y alto que vigilan la implementación de estas políticas, y todo el personal cuyas actividades son gobernadas por éstos. El logro de la misión depende en gran parte en la ética de trabajo, la moral y la productividad de todos los involucrados.

### Medición de la eficacia y la eficiencia en la utilización de recursos

**Definiciones.** Para ser *eficaz*, una organización tiene que lograr avances satisfactorios respecto al cumplimiento de sus fines y objetivos. Sin tomar en cuenta unas pequeñas excepciones, la misión principal de cualquiera organización

## Gestión de Inteligencia en las Américas

de inteligencia es *satisfacer las necesidades de sus clientes*, es decir, entregar la *cantidad y calidad* de inteligencia útil y a tiempo a los *clientes*.

Así lo es, si estos clientes son hacedores de política pública a nivel nacional, comandantes militares, planificadores, o cualquier otro. Para ser, al mismo tiempo eficiente, una organización debe satisfacer esas necesidades de sus clientes de manera rentable, conveniente y altamente productiva, con un mínimo de derroche en esfuerzos o recursos. Por lo tanto, se puede decir que, mientras que la eficacia se mide por los resultados obtenidos, la eficiencia se mide por la forma en que se logran estos resultados. Esto significa que la eficacia impacta directamente el cumplimiento de la misión, mientras que la eficiencia afecta directamente el costo de llevar a cabo esa misión.

Es muy posible ser eficaz, incluso sin la eficiencia, cuando los suficientes recursos pueden ser dedicados a aliviar un problema. Pero cuando los presupuestos son limitados, pocas organizaciones pueden largamente tolerar la ineficiencia sin control. Tal situación por lo general obliga a la desviación de los escasos recursos de las operaciones cruciales, para mantener el funcionamiento ineficiente(s). Estas operaciones cruciales pueden, a su vez, estar forzando a su personal a trabajar aún más duro de lo habitual, para estar al día. Pero incluso esto representa sólo una solución a corto plazo, por lo que entonces este curso de acción no puede ser mantenido indefinidamente.

**Criterios de medición.** Para medir qué tan bien una organización está funcionando, en términos de capacidad de cumplir su función con base en los recursos disponibles, tenemos que responder una serie de preguntas. De esta manera, podemos no sólo determinar si la organización es eficiente y eficaz, sino también, si existe algún problema que vaya reduciendo la eficacia y/o la eficiencia, que tal vez pueda ser aliviado con recursos adicionales. Y, si éste es el caso, podríamos usar los resultados de esta investigación como base para documentar la necesidad de recursos adicionales como una propuesta de apoyo financiero.

Ya que este ensayo trata específicamente de recursos de inteligencia, nosotros asumiremos que la organización está evaluada en el terreno de la inteligencia. Empezaremos por plantear cuatro preguntas y explorar sus posibles respuestas. Después interpretaremos el significado de cada una. Debemos tener en cuenta, en la medida que avancemos, qué factores varios pueden afectar la

eficacia y la eficiencia. Nuestro fin no es sólo identificar estos factores en su sentido negativo, sino también considerar posibles soluciones para esos que son adversos.

**Pregunta 1. ¿Ha identificado correctamente la organización a sus clientes?** La mayoría de las organizaciones contestarían afirmativamente. Mientras que es absolutamente posible que una organización ignore algunos clientes potenciales, esta debería, al menos, ser capaz de documentar al menos un cliente válido que necesite de sus productos y servicios. Los clientes no necesitan necesariamente ser los responsables políticos o los militares de alto nivel (los consumidores finales de la inteligencia). En realidad pueden ser otros organismos de inteligencia que necesitan esta información para realizar el análisis, la producción, o cualquier otra tarea, como parte de sus operaciones.

Una *respuesta negativa* a esta pregunta es una alerta. Cualquier organización de inteligencia que no ha claramente identificado a sus clientes podría estar en dificultades para prevenir reducciones durante épocas de austeridad, y de no sobrevivir incluso en condiciones de ajustes financieros muy severos. Después de todo, si no haya nadie que demande la producción informativa de la organización, ¿Quién se quejará si esa producción se reduce o se elimina?

Algunos lectores de este ensayo declararán que lo que motiva las operaciones de una organización de inteligencia no son los clientes, sino su *misión*. Dirán que, siempre que la agencia satisface la(s) misión(es) sujeta(s) para ello en la ley, por una orden ejecutiva, o por algún otro tipo de directiva o mandato, la agencia está actuando con eficacia. Esto es cierto sólo en la medida que la misión original que descansa en un mandato legal siga siendo válida. En la medida que el mundo cambia, así, también, las políticas y las prioridades de los líderes políticos y comandantes militares. Del mismo modo, también lo hacen las necesidades de los consumidores de inteligencia. Así que, independientemente de la intención del mandato, a menos que haya todavía clientes regentados por la inteligencia, la eficacia de la organización no se puede medir únicamente en esos términos.

*Corolario a la Pregunta 1.* De igual importancia a la identificación de quienes son sus clientes, cabe la necesidad de mantener un listado de éstos actualizado. Es necesario revisar esta lista continuamente para tomar en cuenta los cambios cada vez que nuevas organizacio-

## Gestión de Inteligencia en las Américas

nes se crean, se eliminan, se les cambia de nombre, se reorganizan, o se consolidan.

**Pregunta 2. Ha la organización determinado, ¿cuáles son las necesidades de sus clientes?**

Incluso sin saber exactamente lo que sus clientes necesitan, una organización puede, por suerte, proporcionar inteligencia útil. Es muy probable, sin embargo, que la organización pierda su valioso tiempo, esfuerzo y recursos en producir inteligencia de poca o ninguna utilidad para cualquier cliente. Por no haber demostrado una clara necesidad de sus productos, una organización de inteligencia puede hacer que se vuelva vulnerable a los recortes, o aún a la eliminación.

*Corolario a la Pregunta 2.* Igual como en el caso del primer corolario, una actualización del listado de las necesidades del cliente es vital para una eficaz operación de inteligencia.

**Pregunta 3. ¿Está la organización satisfaciendo las necesidades de sus clientes?** Desde el punto de vista de la *eficacia*, esta es una *pregunta fundamental*. Asumiendo que la organización ha identificado a sus clientes y sus necesidades informativas, *la eficacia depende del grado de éxito logrado en satisfacer esas necesidades*. La única manera para determinar esto es a través de la retroalimentación recibida del cliente. La eficacia puede mejorarse considerablemente si se hacen ajustes, basados en la misma retroalimentación.

**Pregunta 4. ¿Está la organización satisfaciendo las necesidades de sus clientes de una manera rentable y eficiente?** Aquí, vamos *más allá de la eficacia*, para dar atención al concepto de la *eficiencia*. Aunque este aspecto quizás no sea fundamental en períodos de abundantes recursos, se hace más y más importante cuando carecemos de fondos. La siguiente comparación ilustra bien esta importante distinción entre la eficacia y la eficiencia:

La entidad más afectada, y el juez último más importante, respecto de la existencia de *eficacia* en una organización de inteligencia es el *cliente*. La entidad más afectada por su *eficiencia* es la *organización misma*. Los jueces últimos para medir la eficiencia de esta organización son los funcionarios que revisan y aprueban las peticiones para fondos sometidas por la organización, y son éstos los que evalúan la manera en que la organización utiliza sus recursos.



**El análisis de las respuestas.** Cada una de las cuatro preguntas sólo se ocupa de un aspecto específico del funcionamiento de una organización de inteligencia en la medida que se identifica la satisfacción de las necesidades de sus clientes. A continuación, se presenta en la siguiente evaluación las implicaciones de las respuestas positivas y negativas a estas preguntas:

*Respuestas a todas las cuatro preguntas ... SÍ*

Desde el punto de vista de gestión de recursos, la organización es exitosa y debería estar en una fuerte posición competitiva para asegurar y mantener control de los recursos que ésta necesita.

*Respuestas a las Preguntas 1-3 ... SÍ*

*Respuesta a la Pregunta 4 ... NO*

Si nos interesa solamente la eficacia, podemos sentirnos satisfechos con los resultados y terminar nuestra reexaminación de la organización. Si, por el contrario, nos encontramos en un entorno donde los recursos financieros son escasos, probablemente desearíamos examinar las razones debidas a la falta de eficiencia de la organización para tomar medidas correctivas.

*Respuestas a las Preguntas 1 y 2 ... SÍ*

*Respuestas a las Preguntas 3 y 4 ... NO*

Este es el *principal caso* para un estudio más detallado. El organismo tiene que detectar la razón por la cual está fallando en satisfacer adecuadamente las válidas necesidades de los clientes, y después tomar medidas apropiadas para remediar la situación.

*Respuesta a la Pregunta 1 ... SÍ*

*Respuestas a las Preguntas 2-4 ... NO*

La organización debe trabajar con sus clientes para desarrollar y mantener al día el listado de requerimientos. Al cumplir esta tarea, se debe evaluar la capacidad del organismo para satisfacer estas necesidades y el grado de eficiencia con que se logra esto.

*Respuesta a la Pregunta 1 ... NO*

Si la organización no sabe quiénes son sus clientes, ¿cómo podría identificar sus necesidades o determinar si están satisfaciendo algunas de estas necesidades? La posición competitiva de la organización es muy débil, en términos de capacidad de conseguir recursos nuevos y mantener control sobre los recursos que ya tiene.

Los factores que pueden impedir el logro de la eficacia y/o la eficiencia. Si la organización ha determinado que conoce a sus clientes y cuales son sus necesidades, pero no es capaz de satisfacer estos requerimientos, se debe hacer un esfuerzo para determinar las causas subyacentes de esta debilidad. De todas las razones posiblemente responsables de esta falla, las siguientes son las causas más probables. No obstante la complejidad de la situación, las insuficiencias generalmente se encajan dentro de uno de tres tipos principales:

*Liderazgo / deficiencias gerenciales.* Estos involucran problemas, tales como una mala planificación, conflictos de personalidad, luchas internas, falta de comunicación, políticas inapropiadas o contraproducentes, procedimientos ineficientes, moral baja, malas relaciones interpersonales entre empleados, ambiente de trabajo hostil, etc.

*Debilidades estructurales.* Aquí son incluidas cosas tales como un sistema de organización que no funciona, cadenas de responsabilidad confusas, operaciones internas engorrosas e ineficientes, inadecuada distribución física de las instalaciones, condiciones de trabajo inseguras o físicamente no confortables, falta de interacción con entidades externas, etc.

*Deficiencias de recursos.* Estas son la escasez de fondos para operar, para compra de equipo o para emplear personal. Ya sea real o percibido, éste es el problema más común mencionado por la mayoría de organizaciones como la causa principal de su incapacidad para satisfacer las necesidades de sus clientes.

### Cómo superar la falta de eficacia y de ineficiencia

**Búsqueda de remedios.** Ahora vamos a dirigir nuestra atención de los problemas a las soluciones, mientras exploramos las maneras más apropiadas para superar las debilidades descritas con anterioridad. No todos estos remedios pueden, o deberían incluir recursos adicionales. De hecho, en muchos casos, la organización cuenta con todos los recursos que necesita para resolver sus problemas, pero sus líderes no están al tanto de la verdadera naturaleza de estos problemas o no están dispuestos a tomar las medidas necesarias para solucionarlos. Sin embargo, existen otros remedios que, de hecho, dependen de asistencia externa, ya sean fondos o asesoría por parte de expertos.

Consideraremos cada uno de los tres tipos de problemas mencionados arriba, y discutiremos sus soluciones.

**Liderazgo o remedios gerenciales.** Ya que este tipo de problema es *interno* a la organización – usualmente causada por las personalidades, por la burocracia, por la cultura institucional, o por otra causa similar, casi siempre *debe ser resuelto internamente*. Esta solución requiere que el liderazgo de la organización tome los riesgos necesarios para permitir que el cambio se lleve a cabo. Además, el personal de todos los rangos administrativos debe estar dispuesto a participar en el proceso de cambio. Esto es apropiado si los pasos correctivos fueron determinados a través de medidas internas o recomendaciones de consultores externos de gestión.

Organizaciones que sufren de problemas de liderazgo o gerenciales regularmente ignoran lo obvio e insisten en buscar soluciones a través del proceso presupuestal. Sin embargo, los que revisan las propuestas para fondos adicionales de estas organizaciones pueden ser escépticos en que ese dinero adicional resolverá el problema. En tal caso, los revisores examinarán las peticiones con mucho cuidado y buscarán evidencia de exactamente cómo serán usados los fondos adicionales para resolver el problema.

**Remedios para los problemas estructurales.** Problemas estructurales (de la organización) pueden ser causados por fuerzas ya sean internas, externas, o una combinación de las dos. Para resolverlos, la organización tiene que identificar las características y el alcance del problema, tomar acciones internas para solucionar el problema (en la medida de lo posible), y trabajar con otras organizaciones para hacer frente a los aspectos comunes del problema.

Es posible que, incluso si todas esas medidas son tomadas con éxito, puedan ser necesarios algunos recursos financieros o de personal adicionales. Si es así, las solicitudes de estos recursos adicionales en el presupuesto pueden ser fortalecidos al mostrar como éstos complementarán las medidas correctivas que ya se han tomado para resolver el problema.

Una excelente manera para hacer esto es establecer y mantener una *arquitectura de inteligencia* que identifique las capacidades actuales y deseadas, los roles y misiones organizacionales, las interrelaciones funcionales, y otras características de un “plan maestro” de inteligencia. Algunas arquitecturas

se sobreponen, ya que abordan cuestiones que requieren la cooperación y la interacción entre múltiples organizaciones, comandos y agencias. Al trabajar juntos para resolver los problemas de interés común, una serie de organizaciones individuales puede formar relaciones simbióticas. Ellos pueden poner en común sus recursos, actuar como cajas de resonancia a las ideas de los demás, y compartir los frutos que eventualmente brotan de estos esfuerzos. Por lo tanto, una coordinación a escala conjunta de las arquitecturas es una manera mucho más eficiente y eficaz de conseguir los resultados deseados que tener cada organización que procurar aplicar su estrategia de arquitectura de forma aislada.

**Remedios presupuestales.** Si una organización determina que su ineficacia verdaderamente es debido a la falta de recursos, el proceso presupuestal sería la manera apropiada para la búsqueda de una solución. Recursos financieros o de personal adicionales podrían ser buscados a través de esfuerzos de programación y presupuestación. Recursos financieros también podrían buscarse en el corto plazo a través de acciones de reprogramación o una solicitud de fondos adicionales. Los administradores de recursos de la administración deben trabajar con el personal asignado de las oficinas que sufren el déficit. Juntos, determinarán cuáles recursos financieros y/o de personal necesitan las oficinas para superar las deficiencias, y luego desarrollar la descripción del proyecto, la justificación que lo sostiene, y el perfil de costos (es decir, la relación de recursos requeridos) que se incluirán en la propuesta. Una vez que la propuesta haya sido finalizada y presentada para su consideración en el proceso presupuestal, los administradores de recursos la seguirán a través del sistema de gestión de recursos. Este camino conducirá, con suerte, hasta la inclusión de los recursos deseados en el aprobado presupuesto nacional.

En los Estados Unidos, la adquisición de estos recursos es a través del proceso presupuestal que por lo general requiere un mínimo de dos años. Hay, sin embargo, fuentes alternativas de fondos, que no requieren involucrar tal tiempo y proceso, a saber: a) Fondos del presupuesto actual de una oficina que pueden estar a disposición de otra oficina que los necesite para abastecer un requisito-sin-fondos (RSF); b) Acciones de reprogramación que traen a la organización recursos adicionales desde otra organización; y c) Apropiaciones suplementarias. Si bien cada uno de ellos es una fuente potencial de financiación a corto plazo, ninguno podría ofrecer una solución para resolver un déficit que requiere sostenibilidad durante muchos años. Además, los fondos recibidos a

través de la segunda y tercera fuentes son generalmente diseñados para llenar los requisitos específicos que ya han sido identificados en el momento en que el dinero llega a la organización. La información sobre cómo se pueden buscar los recursos para satisfacer las necesidades en curso se discutirá más adelante en este ensayo. Lo que se presenta debería ser útil tanto para los administradores de recursos quienes trabajan el proceso presupuestal, como para los profesionales de inteligencia que quieran ofrecer a los administradores de recursos la más alta calidad de información para ayudar en la búsqueda de los recursos que necesitan los profesionales de inteligencia para llevar a cabo sus misiones.

### Gestión de la propuesta de presupuesto

Si una organización está buscando financiación para un nuevo requerimiento o reuniendo sus datos para un proyecto de presupuesto anual, la documentación requerida contendrá los mismos componentes básicos (ya sea para un solo requerimiento nuevo o por cada dato individual en la propuesta anual). Estos componentes son: a) Una descripción clara de lo que se necesita y como será desarrollado y empleado; b) Una justificación del por qué esto es necesario y qué puede esperarse que suceda si no se cumple el requerimiento; y c) Un resumen de los recursos que establecen los costos proyectados a través de los años y que son necesarios para satisfacer el requerimiento. Una propuesta efectiva presenta una imagen clara y completa del requerimiento y de la manera en que la organización tiene la intención de satisfacerlo, y presenta esa visión en un estilo que puede ser entendido claramente por cualquier persona que deba leerla o revisarla. Cuanto más se entienda a cerca de los fundamentos básicos de desarrollo y comercialización de una propuesta de financiación, mayor será la posibilidad de éxito en la adquisición de los recursos necesarios. Una descripción vaga e incompleta del requerimiento puede afectar seriamente una propuesta de financiación. Con esto en mente, podemos ahora examinar las medidas a seguir en el desarrollo de una solicitud de fondos de alta calidad y que tiene todos los ingredientes necesarios.

### *Adaptando la solicitud para la audiencia*

Es importante tener en cuenta a todos aquellos que estarán involucrados en el proceso de revisión y aprobación a través del cual pasará la propuesta en su camino hacia la aprobación final. Esto significa que las descripciones y justificaciones de los proyectos deben ser apropiadas para la cadena de aprobación a

## Gestión de Inteligencia en las Américas

través de la cual viaja la propuesta. Cuanto más alto es la jerarquía del revisor en esta cadena de aprobación, mayor será la probabilidad de que él o ella carecerán de los antecedentes y experiencia para entender los detalles muy técnicos y especificaciones (más adelante se hablará acerca de cómo manejar esta situación).

En el caso de un proyecto asociado con un activo de la inteligencia militar táctica, tendrá que hacer frente a diferentes problemas que a uno que es más de naturaleza estratégica. Dado que estas propuestas, sin duda, pasarán a través de diferentes cadenas de aprobación, cada una debe ser presentada de tal manera que pueda ser entendida por todos aquellos que participan en su revisión/aprobación. Y en cada caso, es muy probable que haya oficiales, tanto militares como civiles, en el proceso de revisión con diferentes antecedentes, experiencias e intereses.

**Desarrollando y articulando un concepto.** El punto de partida para la creación de una propuesta es identificar exactamente lo que se necesita y cómo el proyecto se ajustará a la operación en curso, siempre y cuando sea aprobado e implementado. Es particularmente importante anticipar el impacto que su implementación tendrá sobre las cargas de trabajo existentes para los empleados, los equipos, el espacio y las instalaciones. Esto requiere que la persona que presenta la propuesta deba usar dos tipos de pensamiento crítico: 1) global y 2) estratégico (o programático). Ahora, vamos a examinar cada tipo y estudiar las implicaciones de cada cual.

**Pensamiento global.** Los que emplean este tipo de pensamiento consideran el alcance total de la necesidad, no sólo de sus ingredientes básicos, sino de todos los recursos requeridos - para cumplir plenamente lo que debe hacerse para alcanzar el fin deseado. Ellos consideran factores tales como suministros, equipo, mobiliario, servicios, construcción o renovación de instalaciones, viajes, capacitación, etc. El pensamiento global también requiere la ponderación de las posibles compensaciones que pueden afectar los costos y la viabilidad del proyecto. Esto incluye factores tales como la compra frente al arrendamiento, y el uso de contratistas frente a nueva mano de obra (y en el caso de nueva mano de obra, si debe ser militar o civil). Gracias a este tipo de pensamiento, el autor de las iniciativas propuestas trata de anticipar cualquier cosa que podría forzar ajustes en las operaciones una vez que el proyecto está en ejecución.

**Pensamiento estratégico / programático.** Aquí, hay que considerar las implicaciones presupuestales de las necesidades, a mediano y largo plazo, más allá

de los costos iniciales de implementación. De especial interés, son los costos a ser incluidos en presupuestos futuros, como reemplazo, repuestos, mantenimiento, y reposición de equipo mayor y de sistemas. Para pensar estratégicamente, hay que tratar de: a) anticipar todos los costos asociados con el establecimiento de una capacidad; b) reducir al mínimo la posibilidad de costos extras durante la implementación que sobrepasen la cantidad aprobada; y c) asegurar que, al finalizar la implementación, la capacidad esté funcionando de tal manera que satisfaga o exceda las expectativas.

### *Redactando la propuesta*

Independientemente del exacto formato usado por una determinada organización, una propuesta de financiación contiene cuatro componentes fundamentales: una descripción del programa deseado, una justificación, una declaración del impacto, y un perfil de costos. A continuación una explicación de cada uno de estos componentes.

**Descripción del programa.** He aquí donde comienza la parte narrativa de la propuesta. Se debe comenzar con un breve listado de categorías específicas de recursos a ser adquiridos, tales como el personal (es decir, posiciones militares y/o civiles y/o apoyo de contratistas); suministros, equipo, muebles, y similares (computadores y equipo electrónico, bienes fungibles, equipos de comunicación, televisores y muebles de oficina); servicios (diseño y desarrollo de software, la recolección y análisis de inteligencia, capacitación del personal, el diseño y desarrollo curricular, servicios de consultoría, etc); la construcción o renovación de instalaciones y, por último, cualquier otra cosa que pudiese ser financiada a través del proyecto, como los viajes y los viáticos, compra de licencias de software, el arrendamiento de las líneas de comunicaciones, y las horas de vuelo para misiones de reconocimiento aéreo. A continuación, debe presentarse una breve exposición de los fines perseguidos por la que los recursos han de ser adquiridos.

La mayor parte de la descripción debe ser una explicación detallada de cómo se utilizarán los recursos que se pretenden usar para el logro del propósito previsto por el proyecto. Debe ser lo más exhaustivo, pero conciso y breve en lo posible, y debe incluir un calendario de ejecución y las principales limitantes. Para ser eficaz, la explicación debe demostrar un pensamiento programático, es decir, una comprensión clara de lo que se requiere para iniciar y llevar a cabo plenamente la capacidad de propuesta. La descripción debe ser clara,

## Gestión de Inteligencia en las Américas

concisa, y al grano, evitando el lenguaje excesivamente técnico con una jerga llena de siglas y abreviaciones (Sería muy buena idea ofrecer las palabras completas cada vez que una sigla o abreviación aparezca por primera vez.). La descripción debe ser capaz de ser entendida por los revisores en todos los niveles de la cadena de aprobación. En el caso de ser útil proveer detalles muy técnicos para los revisores suficiente familiarizados con tal información, éstos se pueden presentar en un párrafo distinto más tarde en la sección narrativa, o en un apéndice o documento adjunto. Todo en la parte expositiva debe ser internamente coherente y con pleno apoyo de los números en el perfil de costos (que se describirá más adelante).

**Justificación.** La justificación identifica la necesidad fundamental de la misión, las razones por las cuáles se necesita el proyecto así como una explicación del impacto anticipado de no ser aprobado ni financiado el mismo. La *necesidad de la misión* se refiere a fines y objetivos identificables que serán sostenidos gracias a la capacidad solicitada y/o cómo el proyecto responderá a la orientación de alto nivel dirigida a la organización. Para ser eficaz, una justificación tiene que ser escrita de tal manera que convenza a los evaluadores que el proyecto y el gasto de recursos verdaderamente valen la pena, y que el proyecto representa *el mejor de todas las opciones o alternativas* disponibles para el logro de la misión establecida.

**Declaración del impacto.** Ya que la justificación explica los beneficios ofrecidos por el proyecto, la declaración del impacto indica el costo de no aceptar y financiar el proyecto. Explica los efectos negativos que resultarán si no se encuentran los fondos necesarios para el proyecto. Una declaración del impacto también explica las *implicaciones o ramificaciones* de este impacto negativo sobre la seguridad nacional, al apoyo a fuerzas militares en combate, o algún otro interés fundamental. La declaración va más allá de las circunstancias negativas que probablemente resultarán de la no aprobación del proyecto, a las razones por las cuales los evaluadores deben interesarse por este suceso. En algunos casos, el impacto negativo puede ser la falta de aprovechar los ahorros cuantificables en dinero, personal, o tiempo, si el proyecto no es aprobado.

**Perfil de financiamiento.** Este es el *resumen de recursos*, en la forma de una tabla/cuadro de datos en la cual se presentan los *costos financieros y de personal* del proyecto. En la parte de arriba estarán los costos financieros para cada año fiscal en el que estaría el financiamiento requerido, y en la sección inferior



están los datos del personal (en términos de números de posiciones militares y civiles). Estos datos serán exhibidos en la tabla siguiente (asumiendo que los costos financieros se desglosan por categorías de asignación, como se hace en el Departamento de Defensa de los Estados Unidos).

Tabla 11 Planilla de Resumen de Recursos de Inteligencia					
Categoría	Año Fiscal 2	Año Fiscal 3	Año Fiscal 4	Año Fiscal 5	Año Fiscal 6
O&M					
Obtención					
IDP&E					
ConMil					
PersMil					
Costo Total					

Oficial					
Incorporado					
Civil					
Personal Total					
O&M=Operación y Mantenimiento; IDP&E=Investigación, Desarrollo, Prueba, y Evaluación; ConMil=Construcción Militar; PersMil=Personal Militar					

Fuente: Creado por el autor.

Los costos presentados en el perfil deben ser explicados, en una breve descripción antes o después de la tabla. Esta técnica dará a los evaluadores una base para determinar si los datos de la tabla son razonables, ya que se les explican los factores que fueron usados en la preparación de las cifras para cada celda de la tabla. Esto es especialmente importante con datos financieros compuestos de gastos múltiples de la misma categoría. La intención es otorgar a los evaluadores de la propuesta una idea mucho más clara de lo que va a ser comprado durante cada año. Esto podría proteger a la propuesta de recortes arbitrarios, ya que los evaluadores serán capaces de medir el impacto que causaría un recorte al proyecto.

### *El mercadeo de la propuesta*

Debe ser claro, en este punto, que el desarrollo de una propuesta de financiamiento en conjunto requiere de mucho tiempo y energía personal. Pero el trabajo no termina ahí. Incluso si la propuesta está clara y construida correctamente, los oficiales encargados de la gestión de recursos no pueden bajar los brazos y dejar el destino del proyecto en manos de la Providencia. Ellos tienen que participar directamente en el proceso de revisión para entender profundamente la propuesta. Hay que dotar a la propuesta del más transparente proceso posible en la etapa en que se formula el presupuesto financiero anual. Después de todo, nadie sabe mejor que el gestor de la propuesta lo que el proyecto es capaz de hacer y lo mucho que puede beneficiar a la organización.

Paralelo a la propuesta está el mercadeo que toma lugar en todos los niveles de la organización, como parte de la competencia entre supervisores de nivel intermedio, que se esfuerzan en ganar el favor de sus superiores gracias a la aceptación de los proyectos. A su vez, los jefes de división, compiten por ganar el favor de los individuos y grupos con liderazgo como parte del proceso de deliberaciones y de toma de decisiones. En muchos organismos, los datos y cifras extraídos de propuestas por escrito se resumen en “tablas de diagramación” usadas en sesiones de información formal e informal, y, eventualmente, en presentaciones que toman lugar en reuniones de decisión. Todo esto se hace con el propósito de seleccionar, de entre una amplia gama de proyectos, algunas “piedras preciosas” dignas de consideración por la jefatura, para ser incluidas en el programa presupuestal final de la organización. En fin, los líderes de más alto rango seleccionarán los proyectos que a su juicio ofrecen la mejor oportunidad para lograr las prioridades del director o del comandante.

### **Principios presupuestales para supervisores o directores de oficina**

#### *Responsabilidades de los supervisores de recursos*

Los que gestionan o dirigen actividades funcionales proveen generalmente a especialistas en recursos muchos de los datos que se usan para preparar y justificar propuestas financieras. Si se dan cuenta o no, todos los supervisores de los organismos de inteligencia tienen responsabilidades en el área de recursos, incluyendo los siguientes:

**La defensa de recursos existentes.** El proceso presupuestal se ocupa no sólo de la búsqueda de recursos para el futuro, sino también en la defensa de los que forman parte del presupuesto actual. En períodos de disminución o por lo menos de no aumento presupuestal, los únicos fondos disponibles para requisitos nuevos se encuentran dentro del presupuesto de la organización misma. Esta situación dicta que la organización ofrezca ítems en su propio programa aprobado como compensación para fundar algunos de los ítems nuevos en su propuesta del ciclo presupuestal corriente. Pues, gerentes siempre tienen que estar preparados en defender sus recursos actuales para que no sean destinados para el pago de cuentas en otras áreas. La misma preparación resultará útil si tienen que proveer información durante una “convocación de datos”, que suele referirse a un “Por si acaso me roban recursos”. En estos ejercicios, los supervisores tienen que indicar lo que creen vaya a pasar respecto a sus capacidades de operación, si sus presupuestos fueran recortados en una cantidad arbitraria, como del 5 o 10%. En cada una de estas situaciones, todas las oficinas tienen que defender los fondos que ya tienen en sus presupuestos financieros, simplemente para no perder algunos de esos fondos. Por eso, el conocimiento de lo básico del proceso de presupuesto puede ser muy beneficioso, incluso para los gerentes que no hayan previsto la necesidad de buscar recursos adicionales, por lo menos en el momento actual.

**La atención a requerimientos sin fondos.** Todas las organizaciones intentan exigir los recursos presupuestarios (los destinos finales de fondos) en la medida posible, para evitar la pérdida presupuestal para gastos de fondos que hasta el momento no han sido efectuados. Por eso experimentamos a mediano y fin de año, una revisión de la “ejecución” del presupuesto, con el fin de encontrar cualquier fuente presupuestal que probablemente no va a ser ejecutada al final del año fiscal. Estas revisiones generalmente identifican fondos superavitarios en algunas líneas que pueden ser redirigidos a proyectos fundamentales que carecen de fondos. La competencia por este exceso de fondos generalmente involucra un proceso similar al programa anual y a lo usado cada año para formar la propuesta presupuestal anual (pero en este caso, usualmente con poco tiempo para preparar la propuesta). Por eso, los que pueden producir, rápidamente, una propuesta que indica la necesidad de recursos adicionales ocupan buena posición para recoger algo de este exceso de dinero.

**Recurso humano y manejo de personal.** Los supervisores en cada nivel de una organización de inteligencia son responsables del manejo del recurso

## Gestión de Inteligencia en las Américas

humano asignado. Esto incluye actividades tales como: a) revisiones periódicas a reportes que identifiquen deficiencias en la cantidad de personal civil y/o militar, para asegurar que el recurso humano asignado sea el adecuado para cubrir la carga laboral; b) revisiones a las descripciones de posiciones militares y civiles para asegurar que reflejen correctamente los quehaceres de los funcionarios; y c) participación, cuando sea necesario, en la planificación e implementación de reorganizaciones. Estos supervisores también dirigen una amplia gama de actividades asociadas con la gestión de personal, lo que puede afectar la productividad de todos o muchos de los empleados.

**Administrar espacio y equipo.** Normalmente, los supervisores son responsables por la condición física del espacio de trabajo y por todo el equipo alojado en este espacio. Estas responsabilidades tienen implicaciones fiscales, ya que es preciso que haya fondos adecuados en el presupuesto para mantener espacio y equipo, para comprar equipo de reemplazo, y para renovar el espacio de trabajo.

**Contratación.** Los supervisores de una organización tienen un rol crítico en la preparación de los documentos relacionados con contratos para la compra de materiales y/o servicios. Ellos tienen que proveer gran parte de la información requerida por la oficina de contratos para preparar el formulario de declaración de trabajo o declaración de objetivos que acompañará la propuesta de petición a ser publicada a los proveedores que deseen someterse a licitación para ganar el contrato. Mucha de esta información puede ser extraída de la descripción del proyecto incluido en la propuesta original, que fue usado para solicitar los fondos necesarios del proyecto que está siendo implementado por el contrato en cuestión.

**Implementar los planes de gastos.** La mayoría de los supervisores tienen un “plan de gastos”, que es una herramienta usada para mantener un saldo corriente de fondos disponibles, para cualquier parte del año fiscal. Esta herramienta ayuda al gerente a cumplir sus quehaceres relacionados con asegurar que hay, en cualquier momento, suficientes fondos en el presupuesto para: a) Pagar todos los gastos anticipados durante el año y b) Evaluar el impacto potencial de las necesidades de financiación no previstas y que surjan durante el año. Su uso principal es alertar al gerente de deficiencias potenciales que podrían requerir fondos adicionales o forzar la terminación o disminución de ciertas actividades planeadas. Una manera en que los supervisores pueden

medir la capacidad de sus subordinados en su propia gestión de gastos del plan de presupuesto es hacer el seguimiento a los compromisos, las obligaciones y el desembolso de fondos.

### *Visión estratégica*

Cada supervisor y gerente de oficina de inteligencia está obligado a tratar de establecer una familiaridad funcional con el aparato y los procesos de gestión de recursos de su país. También, estos oficiales tienen que desarrollar un estilo apropiado para negociar la inevitable política burocrática que acompaña la competencia por fondos adecuados destinados a programas de inteligencia. Al mismo tiempo, necesitan saber cómo dialogar con los colegas quienes controlan la asignación de personal y espacio/provisiones, el uso ocasional de servicios contratados, y otros recursos que pueden afectar la capacidad de cumplir las misiones y responsabilidades asignadas. Hablando de tales responsabilidades, no olvidemos la importancia de entender el lado substantivo de la empresa de inteligencia. Es decir, se necesita saber el papel fundamental del presupuesto para el alcance de las misiones de la organización, y la necesidad de gastar recursos financieros de la manera más eficaz y eficiente posible. Desde la perspectiva de las vivencias del autor, los principios y las prácticas descritas aquí son indispensables para responder a este reto de enormes proporciones.

### Epílogo

Al iniciar este ensayo, el autor enfatizó la importancia para los especialistas de la gestión de recursos de inteligencia de mantener su experiencia en el tema. Ahora, la información que aquí se presenta con énfasis en los principios vigentes, debe ayudar al lector a apoyar este objetivo.

Esta información debe ser aún más útil como una guía básica para el personal asignado a las oficinas responsables del desarrollo y ofrecimiento de propuestas y planes presupuestales. Se dieron ejemplos de propuestas presupuestales eficaces y los criterios específicos para medir la eficacia de una propuesta. Esta información debe ser útil, no sólo para las oficinas que preparan propuestas, sino también para el personal responsable de revisar éstas. A pesar de todas las buenas intenciones, cualquier persona responsable de revisar y hacer las recomendaciones que determinarán la respuesta a las propuestas financieras, debe tener un útil y completo juego de herramientas para poder juzgar los diversos aspectos de las propuestas y determinar la calidad de éstas. La eficiencia y eficacia del uso de recursos requiere de la atención de toda persona en la cadena de gestión de recursos, porque, al fin de todo, la última fuente de fondos y la razón entera para la existencia de un sistema nacional de seguridad e inteligencia son uno solo - nuestros conciudadanos quienes no sólo necesitan sentirse seguros, sino estar seguros, mientras que persiguen sus sueños de soberanía.

### Biografía del autor

**Dan Elkins**, experto reconocido nacionalmente en la gestión de los recursos de inteligencia. Es un oficial naval de inteligencia jubilado, con experiencia militar en criptología, inteligencia de imágenes, planificación de recursos y de personal, gestión y coordinación de la reserva militar, y entrenamiento y educación de inteligencia. Durante más de dos décadas, él ha dictado clases en gestión de recursos para el *Defense Intelligence College* y su sucesor institucional (ahora la Universidad Nacional de Inteligencia) y también en el Centro Conjunto de Entrenamiento Militar de Inteligencia en Washington, DC. En febrero de 1995, estableció la *DWE Enterprises*, una compañía en consultoría sobre la gestión de recursos de inteligencia, y ha servido como miembro de la facultad de la Academia de Inteligencia y Seguridad. El señor Elkins ha impartido enseñanza a más de 10,000 personas de la Comunidad

## Russell G. Swenson y Carolina Sancho Hirane

de Inteligencia y del Departamento de Defensa de los Estados Unidos, los cuerpos administrativos de varios comités del Congreso, dos laboratorios nacionales, y varias empresas privadas. Él recibió su B.A. en español en 1975 y su M.B.A. en Finanzas en 1980, de lo que es ahora la Universidad de Massachusetts en Lowell. Es el autor de las ediciones 2004, 2006, 2010 y 2014 del libro *Managing Intelligence Resources* (Gestión de Recursos de Inteligencia-DWE Press), la referencia bibliográfica más examinada del país en el área de la gestión de recursos de inteligencia y defensa. Correo electrónico: [dwelkins2@cs.com](mailto:dwelkins2@cs.com).

## Cooperación en Inteligencia en el Marco de la Unión de Naciones Suramericanas (UNASUR): Posibilidades y Limitaciones

Carolina Sancho Hirane

*Axelrod al hablar de cooperación comienza con una pregunta clave "¿En qué condiciones emergerá la cooperación en un mundo de egoístas sin una autoridad central"?<sup>431</sup>*

*Los países europeos van asumiendo progresivamente que los riesgos y amenazas ya no son diferentes para cada país sino que son transnacionales, y que los riesgos compartidos sólo pueden enfrentarse con soluciones comunes.<sup>432</sup>*

La cooperación en inteligencia en organismos multilaterales es consecuencia de amenazas y riesgos a la seguridad de los países que forman parte de estos organismos y su finalidad es generar una capacidad preventiva para evitar la realización de aquellos riesgos y amenazas que en forma consensuada han sido definidos como un peligro a la seguridad de los países miembros. Al considerar que la cooperación en inteligencia puede concretarse de modo formal e informal, como también, que ésta entre países de UNASUR es realizada en el marco de otros organismos multilaterales de cooperación en inteligencia, se constata que en el marco de UNASUR la cooperación en inteligencia de algún modo existe<sup>433</sup> y hay muchas acciones por realizar para mejorarla en términos cualitativos y cuantitativos.

Para estos efectos, y para consideración de la gestión de inteligencia desde el poder ejecutivo de los gobiernos respectivos, se ha buscado hacer una aproximación a las posibilidades y limitaciones de cooperación en inteligencia en el marco de UNASUR. En este sentido junto a las posibilidades de concreción de esta práctica, son identificados los requisitos que es necesario cumplir para su efectivo desarrollo. La pregunta que ha orientado esta reflexión es "¿Cuáles son los obstáculos a la cooperación eficaz en inteligencia en UNASUR, y cómo pueden ser superados?" Adelantando el resultado de este trabajo podremos identificar requisitos mínimos a cumplir para su realización eficaz.



Este artículo comienza con una aproximación teórica a la cooperación en inteligencia que permitirá una mejor comprensión de sus fundamentos, posteriormente será descrita su tipología obtenida a través diversas aproximaciones académicas sobre la materia, con la finalidad de poder aplicarlas posteriormente al caso de UNASUR.<sup>434</sup>

### Cooperación en inteligencia: aproximación teórica

Desde la teoría<sup>435</sup> se reconoce que entre los países hay cooperación y competencia en materia de inteligencia. En este sentido, los Estados son particularmente reticentes a subordinar sus agencias de inteligencia a los requerimientos extranjeros y siendo ya difícil el debate dentro de un mismo Estado sobre cuánta información el Estado debe tener de sus ciudadanos y compartir entre agencias ejecutivas, decidir cuánta de esa información compartir con agencias extranjeras pareciera ser aun más complejo. No obstante, las relaciones interagenciales se enmarcan dentro de un contexto de procesos burocráticos, y el cómo los distintos servicios procesan y diseminan la información obtenida es una función propia de cada agencia y servicio de seguridad.<sup>436</sup>

La creación de flujos relevantes de información compartida y la coordinación ante amenazas comunes es una capacidad que se construye en el tiempo y en base a las distintas interacciones entre servicios. Asimismo, nuevas amenazas suponen desafíos a estas agencias de seguridad, que en orden de incrementar su eficiencia se ven en la necesidad de compartir información y/o funciones con servicios extranjeros. Generar, profundizar y mejorar estos lazos es uno de los desafíos a la hora de enfrentar amenazas como el terrorismo, el crimen y/o delito organizado, o el narcotráfico, entre otras, que requieren de una profunda y mejorada cooperación entre los servicios de inteligencia para abordarlas en forma efectiva.

La cooperación en inteligencia en el marco de organismos multilaterales no es un tema nuevo. Por ejemplo, la idea de un “servicio de inteligencia de las Naciones Unidas”<sup>437</sup> se planteó en círculos norteamericanos a fines de la guerra fría y debido a las tensiones internas que generaba la creación de este organismo fue descartada la proposición.

Desde esta perspectiva, la idea de cooperación en inteligencia en organismos multilaterales es un tema recurrente, cuando se analiza la manera de enfrentar

## Gestión de Inteligencia en las Américas

en forma eficaz amenazas transnacionales y/o el resguardo de los bienes públicos mundiales.<sup>438</sup> En efecto, comienza a ser frecuente que en numerosas publicaciones se indique la urgente necesidad que tienen los países para cooperar en materia de inteligencia, si el objetivo es enfrentar de modo creíble y con razonables niveles de eficacia y eficiencia las amenazas, riesgos, vulnerabilidades y oportunidades existentes en materia de seguridad de los países. Reforzando la idea del valor de la cooperación en inteligencia para el tratamiento de las amenazas transnacionales, como por ejemplo el terrorismo, se señala que:

la comunidad de inteligencia estadounidense, junto con los servicios de inteligencia extranjeros, deberían trabajar en crear una base de datos que identifique y siga la pista de los combatientes extranjeros, sus asociados conocidos y mentores espirituales. Si dicha base de datos se hubiera creado durante la guerra afgana, Estados Unidos habría estado mucho mejor preparado para la subsecuente campaña terrorista del Al Qaeda.<sup>439</sup>

A lo anterior se adiciona, la experiencia de Hans Blix<sup>440</sup> -quien fue director de la Comisión de las Naciones Unidas para el Seguimiento, Verificación e Inspección de Armas de Destrucción Masiva (AMD) para Irak-, en materia de interacción con servicios de inteligencia y los informes que ellos entregan sobre temas de interés multilateral (específicamente en su experiencia referida a la existencia de AMD en Irak), como también, la obtención de datos e información necesaria para su elaboración. Resultado de lo que le correspondió constatar en el cargo ocupado, él plantea que es insuficiente nutrirse exclusivamente de datos, información y/o inteligencia de los servicios de los países respectivos, por cuanto, los intereses nacionales, pueden ser diferentes a los intereses de la organización (multilateral) y ésta última no tiene herramientas para conseguir sus objetivos y no tiene más alternativa que aceptar lo que se le entrega y a partir de eso, tomar una postura.

Desde su perspectiva, reflexionando en torno a la estructura más adecuada para la efectiva cooperación en organismos multilaterales, la conformación de un servicio multilateral que produzca inteligencia con agentes de servicios nacionales puede generar poca credibilidad a nivel internacional, considerándose por parte de los actores de comunidad internacional que los servicios nacionales están actuando a través del organismo multinacional, afectando de este modo,

negativamente la imagen de profesionalismo que requiere todo servicio de inteligencia, particularmente si se ubica en un organismo multilateral.

Sin embargo, en una etapa inicial de la conformación de una entidad de inteligencia en un organismo multilateral internacional, la participación de funcionarios de los servicios de inteligencia nacionales puede constituir un primer paso en el camino de la cooperación. Una segunda etapa en esta materia puede ser con funcionarios propios de la entidad de inteligencia multilateral, los cuales asesoran a sus autoridades (del organismo multilateral) en los temas de su interés estratégico, de acuerdo a las atribuciones y competencias asignadas. En este sentido, la experiencia de Naciones Unidas en las misiones de Operaciones de Paz, muestra la limitada utilidad de la función inteligencia, de acuerdo a la manera en que ésta ha sido implementada desde una perspectiva organizacional.<sup>441</sup> No obstante, se reconocen positivos avances en su estructuración y ejecución que podrían servir como experiencia para una mayor ampliación del uso de la función inteligencia aplicado a las necesidades de organismos internacionales multilaterales como la ONU.<sup>442</sup>

Aunque existen experiencias de cooperación en inteligencia,<sup>443</sup> que pueden ser extrapoladas y adaptadas al caso de UNASUR, ellas están sin explorar. En este sentido, Ugarte evidencia las posibilidades existentes en este tema al recordarnos uno de los objetivos específicos del Consejo de Defensa Suramericano (CDS) que es “promover el intercambio de información y análisis sobre la situación regional e internacional, con el propósito de identificar los factores de riesgos y amenazas que pueden afectar la paz regional o mundial”.<sup>444</sup> Asimismo, el autor a partir de la revisión de los objetivos del Centro de Estudios Estratégicos de Defensa (CEED) del CDS, reconoce la existencia de una función de análisis estratégico y de *inteligencia estratégica*,<sup>445</sup> en varias de las tareas encomendadas.

En este sentido, es factible la cooperación en inteligencia en el marco de UNASUR, no obstante, ello requiere de un delicado trabajo que revise las posibilidades, limitaciones y formas en que ello pueda concretarse, teniendo en consideración que es condición necesaria para su realización, la existencia de beneficios superiores a los perjuicios que ello puede generar para cada uno de los actores involucrados. Sobre este punto, Julia Pulido recuerda el interesante punto que “si las ganancias relativas conseguidas por cada Estado en el proceso de cooperación de inteligencia no producen a largo plazo una mejora

## Gestión de Inteligencia en las Américas

evidente en la posición relativa de unos sobre otros, ni se plantea este tipo de percepción, entonces sí se puede producir una cooperación efectiva”.<sup>446</sup>

Desde una perspectiva académica, puede observarse promisorias oportunidades en Latinoamérica<sup>447</sup> al constatar comunes intereses en el estudio y tratamiento de la actividad como disciplina en la teoría y práctica. Se genera de esta manera, un primer paso para avanzar en el análisis de las amenazas, vulnerabilidades y oportunidades en los temas de seguridad Suramericanos de los países que componen UNASUR, que puede posteriormente ser la base en la gestión de acciones comunes y multinacionales en la materia.

### Tipologías de cooperación en inteligencia

La cooperación en inteligencia, entendida como la “disponibilidad y la capacidad de diversas organizaciones y profesionales de inteligencia de trabajar juntos para lograr objetivos comunes”,<sup>448</sup> implica considerar que “nunca es *ilimitada* por estrecha que sea la alianza entre los países, o el conjunto de países que la practican”.<sup>449</sup> Asimismo, puede ser abordada desde diferentes categorías de análisis<sup>450</sup> las cuales corresponden a:

A. Naturaleza de formalización en las interacciones, puede ser formal o informal. En este sentido, la informalidad corresponde a la inexistencia de acuerdos, convenios, actas que establezcan el interés institucional de intercambiar información de los servicios de inteligencia según determinadas consideraciones. En la práctica, “frecuentemente la cooperación formal encuentra un modo más flexible de instrumentación en el intercambio de notas entre los gobiernos que comprende, antes que en tratados expresos”.<sup>451</sup> Asimismo, la “cooperación *formal, permanente e íntima*, obviamente rara, requiere una fuerte *comunidad de intereses y de políticas exteriores* entre los países participantes”.<sup>452</sup> Un ejemplo de cooperación formal, corresponde al caso de los delegados o enlaces de un servicio de inteligencia en otro diferente al cual éste pertenece.

B. La cantidad de actores involucrados, puede ser bilateral o multilateral. En este sentido, la “cooperación más frecuente es la bilateral, que tiene múltiples expresiones en todo el mundo .... La *cooperación multilateral*, más rara, supone una alianza estrecha y lazos fuertes entre los países que la suscriben”.<sup>453</sup>

C. La áreas temáticas y/o ámbitos de la actividad del Estado, que corresponden a la identificación de tres ámbitos de acción de los servicios de inteligencia, definido por su objeto de interés. Estos tres ámbitos se explican bajo el supuesto de que “existen al menos tres grandes necesidades que se cubren con sus respectivos tipos de inteligencia: la inteligencia militar, la inteligencia estratégica y la información<sup>454</sup> policial o criminal”.<sup>455</sup> Estos tipos de inteligencia son detallados a continuación y son sintetizados en el esquema, donde son presentados como tipos puros. No obstante, se reconocen matices en cada uno de ellos que pueden hacerlos diferentes a lo indicado, en un momento y lugar determinado (por ejemplo, actualmente en el caso de México, dado que las fuerzas armadas y por extensión la inteligencia militar tiene como objeto de interés el narcotráfico, delito históricamente bajo la responsabilidad de la policía, similar situación puede constatare en el caso colombiano).

Tabla 12 Características Diferenciadoras de los Servicios de Inteligencia Militar, Información Policial e Inteligencia Estratégica			
	Inteligencia militar	Información policial	Inteligencia estratégica
Objeto de su actividad	Amenazas	Delitos	Amenazas y delitos
Bien protegido	Fronteras	Orden público	Seguridad del Estado
Origen de la amenaza	Exterior	Interior	Interior - Exterior
Producto suministrado	Mediato	Mediato	Final
Finalidad de su actuación	Preventiva – reactiva	Preventiva – reactiva	Preventiva
Mecanismos judiciales	No	Sí	A veces

Fuente: Antonio Díaz, Miguel Revenga, Oscar Jaime, y Rafael Martínez, “Hacia una política europea de inteligencia”, *Revista Política Exterior* (España) XIX, no. 106 (agosto 2005).

Desde una perspectiva de la cooperación multilateral en inteligencia, Díaz identifica varios niveles en los cuales puede ocurrir:

- i. “El *macro* nivel, que está basado en acuerdos internacionales o tratados; (...) Implica acuerdos multinacionales establecidos con el objeto de establecer existentes o nuevos marcos para el intercambio multilateral de

## Gestión de Inteligencia en las Américas

información o bien otras formas de cooperación activa entre servicios de inteligencia;

ii. El *meso* nivel, que se encarga de las prácticas operacionales y procesos, (...) engloba la estandarización de métodos de comunicación, confección de informes, regulación y periodificación de reuniones a diferentes niveles y contacto permanente con oficiales de enlace;

iii. El *micro* nivel, que lidia con las investigaciones individuales o acciones sobre casos específicos (...) se refiere a la cooperación o la provisión de información sobre un caso específico; una situación que a menudo será decidida *ad hoc* en el nivel inferior en base a situaciones concretas que se presenten”.<sup>456</sup>

En síntesis de la cooperación en inteligencia, puede ser analizada desde diferentes perspectivas, de acuerdo al nivel de formalidad con la cual se encuentra institucionalizada, la cantidad de actores (en este caso países) que participan en ella y los ámbitos o materias que contempla. La consideración de todas estas categorías permite identificar la densidad de la cooperación en inteligencia, en diferentes zonas geográficas que cuenten con acuerdos de asociación. A continuación revisaremos el caso de UNASUR.

### Limitaciones y posibilidades de cooperación en inteligencia

La cooperación en inteligencia en organismos multilaterales con participación de países Suramericanos, tiene raíces históricas, en el marco del conflicto Este – Oeste<sup>457</sup> en la cual la cooperación entre los países indicados y EE.UU., estuvo fundamentalmente basada en el tema ideológico, es decir, evitar que el comunismo se convierta en opción política en Latinoamérica. Sin embargo, desde entonces hasta ahora se han producido cambios sustantivos en la cooperación en inteligencia entre los países que forman parte de esta zona geográfica. En efecto, como se presenta abajo, la cooperación inteligencia en la Comunidad Andina de Naciones (CAN) y en el Mercado Común del Sur (MERCOSUR) y MERCOSUR ampliado (considera además a países asociados)<sup>458</sup> se observan patrones de cooperación diferentes.

Igualmente, al nivel hemisférico, se observa una hegemonía estadounidense en materia de cooperación en entidades de información e inteligencia, de oficinas u organismos encabezados por sí mismo y en otros casos, operando

con países que forman parte de la Organización de Estados Americanos (OEA).<sup>459</sup> En la medida que funcionarios de los servicios de inteligencia de países Suramericanos puedan llegar a conocerse más directamente, bajo los auspicios de organizaciones tales como por ejemplo la Comisión Interamericana para el Control del Abuso de Drogas (CICAD), el Joint Inter-Agency Task Force-South (JIATF-S), y el Comité Interamericano Contra el Terrorismo (CICTE), existe la posibilidad de alcanzar un grado mayor de confianza mutua. En este sentido, una manera de mejorar cooperación entre ellos es a partir de la generación de instancias de conocimiento entre los representantes de los países y entre sus especialistas y directivos.

Asimismo, también la Unión Europea (UE) ofrece experiencias positivas en materia de organismos multilaterales que enfrentan amenazas comunes (por ejemplo la Oficina de Policía Europea -EUROPOL-, el Centro de Situación, entre otros). A partir de éstos es posible constatar la factibilidad de cooperar en materia de inteligencia en organismos multilaterales. A continuación se hará referencia a la actual experiencia de cooperación en el marco de la UE. En efecto, la experiencia europea servirá para ilustrar las posibilidades actuales de cooperación en la materia, de cumplirse algunas requisitos mínimos, tales como: convergencia de las políticas de seguridad, defensa y relaciones exteriores, junto a la existencia de homogeneidad en las prácticas de seguridad de las agencias y la capacidad profesional de sus funcionarios.

### Unión Europea y cooperación en inteligencia

La historia de la construcción europea tiene su origen primigenio en el intento de que no se volviera a producir un conflicto armado devastador entre europeos. Para eso se controlaron a través de Europa los elementos principales de la industria del armamento: el acero y el carbón, en la Comunidad Europea de Acero y Carbón. Sus inicios se remontan a los años cincuenta y tiene un hito trascendental en 1993 cuando el Tratado de la Unión Europea (TUE) entra en vigencia. Hoy día son 28 los países miembros provenientes de los cuatro puntos cardinales de la geografía política y humana del viejo continente.

La construcción de la capacidad de inteligencia, compuesta de comités, grupos de trabajo e instalaciones de monitoreo, ha sido un proceso de largo aliento, metódico y gradual. A ello se suma otra cualidad esencial en las

## Gestión de Inteligencia en las Américas

actividades de la UE. Todo acto de cooperación, intercambio de información y participación en los diversos organismos comunitarios se realiza sobre la base de la completa y total voluntariedad. Dicho de otro modo, ningún Estado miembro es obligado a prestar su concurso en ningún tipo de iniciativas.

Tanto el Parlamento británico como la propia UE han establecido principios rectores para alcanzar una cooperación exitosa en inteligencia. Según los británicos, los principios son cuatro: 1) Confianza en la inteligencia humana; 2) Consciencia de que inteligencia y política van intrínsecamente unidos; 3) Importancia de la ética y 4) Necesidad de que la UE tenga capacidades conjuntas accesibles a todos. Por su parte, la UE ha elaborado cinco principios para la cooperación en inteligencia: 1) Solidaridad entre los Estados miembros de la Unión; 2) Naturaleza voluntaria de las contribuciones de estos Estados; 3) Clara comprensión de la amenaza terrorista y pleno uso de los análisis de amenazas disponibles; 4) Coordinación entre pilares en apoyo del común objetivo de la Unión de combatir el terrorismo y colaboración con socios relevantes, y 5) El consiguiente respeto a la propiedad y efectividad de las mismas.<sup>460</sup>

Uno de los elementos centrales que subraya la cooperación en inteligencia europea y que se da en el discurso de todos los ámbitos de la vida política, económica, social y cultural europea, aparte de la necesaria voluntad política para cooperar, tiene que ver con las amenazas que debe enfrentar la UE. Las actuales amenazas son transnacionales y no están circunscritas geográficamente, es decir, son globales. La lista de amenazas es variada y van desde el terrorismo islámico, pasando por la migración ilegal, el crimen cibernético, el crimen organizado, hasta el cambio climático, la piratería, la escasez de alimentos, la seguridad de los recursos, las pandemias y las enfermedades.

Por cierto, hay consciencia en la UE que el abordar estas amenazas contribuye a la seguridad económica del continente y que la inestabilidad regional puede poner en peligro los “intereses europeos”, como señala el británico William Shapcott, ex director del Centro de Situación (SitCen), un organismo de análisis estratégico de la UE.<sup>461</sup> Hoy ningún país por separado está en condiciones de hacer frente a los desafíos de un mundo incierto e inestable. Por ello, se constata que a nivel europeo existe la necesidad de consultas y análisis continuos en inteligencia al menos sobre las siguientes temáticas: 1) Seguridad militar; 2) Seguridad económica; 3) Seguridad interna (terrorismo y radicalismo/extremismo, entre otros); 4) Seguridad



tecnológica; 5) Seguridad operativa en el manejo de crisis y de conversaciones de paz y en el caso de guerras y tensiones militares; 6) Contraespionaje, y 7) Seguridad informática.<sup>462</sup>

### *Inteligencia estratégica*

Una de las instancias pioneras en la UE para tratar temas de cooperación interestatal en inteligencia estratégica fue el Club de Berna, creado en 1971. En él se reúnen anualmente los directores de inteligencia de los distintos servicios europeos para establecer la agenda de cooperación concerniente a la seguridad del continente. Desde 1999, comienza a tratarse temas relativos al terrorismo, la interceptación de comunicaciones, la encriptación y ciberterrorismo, y desde el año 2000 se suman cuestiones relativas al rol de las agencias de inteligencia en la integración europea.<sup>463</sup>

### *El Centro de Análisis de Inteligencia de la Unión Europea (EU IntCen)*

El primer organismo permanente destinado al análisis de inteligencia estratégica denominado Centro de Situación (SitCen) fue creado en la década de los noventa en el seno de la Unión Europea Occidental (UEO), una organización de defensa y seguridad formada por los Estados miembros de la UE y de la OTAN que dejó de existir en 2011. La mayoría de sus organismos fueron incorporados a la UE. En 1999 el SitCen fue incorporado íntegramente al ámbito de la UE. Su misión fue “la producción de análisis de inteligencia como apoyo a las políticas europeas”, en palabras de su fundador,<sup>464</sup> misión que se mantiene en la actualidad, sin embargo, actualmente ha cambiado la denominación de la entidad a Centro de Análisis de Inteligencia de la Unión Europea (EU IntCen).

Desde el año 2011 (enero) el Centro de Inteligencia de la Unión Europea (EU IntCen) es parte del Servicio Europeo de Acción Exterior (EEAS),<sup>465</sup> el cual tiene por misión proporcionar análisis de inteligencia, alerta temprana y conocimiento de la situación a la Alta Representante de la UE, como también, al EEAS mismo y a los diversos órganos de decisión de la UE en los campos de la política exterior y de seguridad común (PESC) y política europea de seguridad y defensa (PESD) y en materia de contra el terrorismo, así como a los Estados miembros de la UE.<sup>466</sup>

## Gestión de Inteligencia en las Américas

La importancia del EU IntCen reside en que es el punto de fusión de inteligencia civil y militar, y que también tiene la capacidad para convertirse en operativo ante situaciones de crisis. Este Centro tiene varias funciones. Por una parte, es centro de análisis de situación en tiempo real, también tiene una responsabilidad en la tarea de resguardar la estructura de seguridad interna de la UE. A su vez, posee un papel en el acercamiento y la complementariedad a nivel europeo, debido a que se dedica a redactar análisis sobre las diversas amenazas que afectan a la UE por medio de la recolección de los datos que los distintos servicios de inteligencia de los Estados miembros le hacen llegar.<sup>467</sup>

Uno de los mayores problemas que enfrentó el SitCen fue la resistencia de los servicios de inteligencia de los diversos países a la hora de compartir información. Ése es el motivo de que sólo algunos países de la UE, no los 27 de la época, estuviesen presentes allí con su personal. Sin embargo, debido a que los análisis podían llegar a ser más comprensivos y amplios que aquellos de los servicios nacionales, a los que muchas veces les ha faltado precisamente la visión de conjunto que se puede lograr en el seno de los organismos directivos de la UE ha motivado la participación de los países en esta instancia. Por otro lado, no se puede soslayar que el Centro también ha despertado ciertas sospechas a nivel político. En 2010, el Parlamento Europeo ordenó un estudio para corroborar cómo se puede supervisar mejor las actividades del SitCen, pues hasta ese momento el Centro actuaba sin ningún control democrático.<sup>468</sup> No obstante, el haberlo convertido en el año 2011 en entidad que asesora a la Alta Representante de la UE, da cuenta de cómo ha ganado un prestigio asociado al valor del trabajo que desarrolla para asesorar a la más altas autoridades de la UE.

### *Una agencia europea de inteligencia*

Desde hace años se ha discutido, y no solamente en un plano académico, la posibilidad de que la UE tenga su propia agencia supranacional de inteligencia. Esta polémica se ha encendido cada vez que el continente se ha visto afectado por atentados terroristas de magnitud como los ocurridos en Madrid (2004) y en Londres (2005). Incluso el Parlamento Europeo, a raíz de una investigación sobre la polémica red de escuchas ECHELON,<sup>469</sup> ha señalado que “es inconcebible que los servicios de inteligencia sean la última y única área no afectada por el proceso de integración europea”.<sup>470</sup>

Las primeras ideas surgieron en los años sesenta en el seno de la OTAN, cuando algunos funcionarios plantearon establecer formas más coordinadas de compartir inteligencia en Europa. Sin embargo, la misma dinámica de la guerra fría y las rivalidades entre Estados Unidos y Francia abortaron la idea.<sup>471</sup> Luego de la caída del Muro de Berlín nuevamente apareció el tema en la discusión entre académicos, “su papel, decían, sería el de coordinación pasando del análisis de la información suministrada por otros organismos y servicios de inteligencia extranjeros a posteriormente realizar su propia captación de información”.<sup>472</sup>

Precisamente, los Estados menos desarrollados y más pequeños -entre los que destacan Austria, Bélgica, Grecia e Irlanda- son los que alientan la idea de una agencia europea de inteligencia.<sup>473</sup> Han sido los países pequeños los que se han encargado de reflotar varias veces el tema de una agencia europea. Sin embargo, todo indica que por ahora no habrá una agencia europea, pues los países más grandes, especialmente Alemania, España, Francia, Gran Bretaña e Italia, conocidos en el ambiente de inteligencia como el G5, confían más en sus capacidades nacionales y dudan del efecto positivo de un organismo supranacional. Consideran que sólo terminaría duplicando los esfuerzos nacionales y subsidiando a las agencias de inteligencia de los países más débiles. Otro factor es que sólo 8 de los 28 Estados miembros de la UE poseen un servicio de inteligencia exterior. Y en el caso de los países nórdicos el principal esfuerzo de inteligencia radica en la labor de la policía. Esta falta de criterios organizativos comunes puede hacer muy dificultosa la tarea de compartir inteligencia.<sup>474</sup>

Actualmente la UE presenta un interesante modelo de cooperación en inteligencia, en diferentes ámbitos de esta función de Estado (especialmente estratégica y policial). Aunque como modelo, está en proceso de construcción, ya se puede observar acciones en cooperación a nivel meso y macro, según la tipología de Díaz.<sup>475</sup> La UE lleva un importante camino avanzado en materia de cooperación en inteligencia, resultado de la homologación de políticas de seguridad y defensa entre los países de la UE, como también de la coordinación de éstas dos a nivel de UE. Varias de las prácticas observadas pueden orientar las relaciones de cooperación en inteligencia a los países de UNASUR.

Habiendo hecho una breve revisión al caso de la UE, revisaremos la situación de cooperación en inteligencia en Suramérica, dadas las diversas

## Gestión de Inteligencia en las Américas

organizaciones multilaterales de inteligencia que se encuentran en esta zona geográfica.

### Posibles bases para cooperación en inteligencia en UNASUR

Tal como nos recuerda Ugarte, “hasta el momento no han surgido mecanismos institucionales de cooperación en inteligencia en el ámbito de UNASUR, ni existe cooperación en inteligencia que tenga a dicho proceso de integración como referencia”.<sup>476</sup> Sin embargo, existen al menos cuatro motivos que permiten argumentar a favor de una posible cooperación en inteligencia en el marco de UNASUR.

El primer motivo está referido a la existencia de amenazas, riesgos, vulnerabilidades a la seguridad de los países, como también de oportunidades factibles de cooperación en inteligencia que se desprenden del documento constitutivo de UNASUR, que señala, en su párrafo q:

[L]a coordinación entre los organismos especializados de los Estados Miembros, teniendo en cuenta las normas internacionales, para fortalecer la lucha contra el terrorismo, la corrupción, el problema mundial de las drogas, la trata de personas, el tráfico de armas pequeñas y ligeras, el crimen organizado transnacional y otras amenazas, así como para el desarme, la no proliferación de armas nucleares y de destrucción masiva, y el desminado; la experiencia previa que tiene la mayoría de los países de Suramérica en cooperación en inteligencia, que puede vertirse en el área de UNASUR.<sup>477</sup>

Junto a lo anterior, se adiciona el interés en cooperar en materias de defensa, señalándose en el mismo documento: “s) el intercambio de información y de experiencias en materia de defensa”. Como asimismo en materias referidas a: “t) la cooperación para el fortalecimiento de la seguridad ciudadana, y u) la cooperación sectorial como un mecanismo de profundización de la integración suramericana, mediante el intercambio de información, experiencias y capacitación”.<sup>478</sup>

Un segundo motivo, que permite creer en la factibilidad de la cooperación en los temas indicados está dado por la capacidad de inteligencia que tiene cada uno de los países de la zona suramericana. Se constata que la mayoría

de éstos están en condiciones de cooperar en materia de: inteligencia militar, inteligencia policial o criminal e inteligencia estratégica, por cuanto, existen organismos que realizan esta actividad en la mayoría de los países de UNASUR.<sup>479</sup> El cuadro que se presenta a continuación es elaborado a partir de documentos legales que indican las entidades nacionales que realizan inteligencia como parte de un sistema o comunidad de inteligencia nacional.

**Tabla 13**  
**Miembros de la Comunidad o Sistema de Inteligencia**  
**en cada país de UNASUR**

Tipo de Inteligencia País	Agencia Nacional	Inteligencia Militar	Inteligencia Policial	Cancillería	Inteligencia Financiera
Argentina	X	X	X		
Bolivia		X	X		
Brasil	X	X	X	X	X
Chile	X	X	X		
Colombia	X	X	X		X
Ecuador	X	X	X		
Guyana		X	X		
Paraguay		X	X		
Perú	X	X	X	X	
Surinam		X	X		
Uruguay		X	X	X	X
Venezuela	X	X	X		

Fuente: Elaboración de la autora, 2013.

El tercer motivo, es que todos tienen experiencia de cooperación en inteligencia en alguna de las clásicas dimensiones de la función inteligencia indicadas en el acápite anterior: militar, policial, o estratégica. En efecto, todos los países de Suramérica, en mayor o menor medida participan en diferentes instancias de cooperación en inteligencia, que califican como instancias informales. Aunque esta cooperación no se realiza bajo del marco de UNASUR, los países de esta asociación tienen experiencia en estas prácticas.

## Gestión de Inteligencia en las Américas

En el caso de la inteligencia estratégica, existe el “Foro Iberoamericano de Directores de Servicios de Inteligencia”,<sup>480</sup> que se realizan periódicamente en diferentes países Iberoamericanos. Chile fue sede en Viña del Mar el año 2003. Este tipo de encuentros permite iniciar o potenciar el triángulo conocimiento – confianza – cooperación, aspecto clave para alcanzar una cooperación en inteligencia de carácter formal.

En el caso de la inteligencia policial, las policías cooperan en inteligencia en diferentes instancias, entre las cuales destacan: la Comunidad Latinoamericana y del Caribe de Inteligencia Policial (CLACIP) y la Organización Internacional de Policía Criminal (INTERPOL), que concreta la cooperación en inteligencia a través de intercambio de información entre países, conferencias, seminarios, cursos de capacitación y en la elaboración y promoción de producción de documentos estandarizados para abordar determinadas materias de interés policial.<sup>481</sup> Por ejemplo, Chile participa activamente en estas instancias y cuenta con oficiales chilenos designados que se dedican particularmente a la relación con estas entidades (en Carabineros de Chile y la Policía de Investigaciones de Chile, respectivamente).

En el caso de la inteligencia militar, los países Sudamericanos y el Comando Sur de Estados Unidos forman parte una red denominada “Red Sudamericana de Comunicaciones Protegidas SURNET, instrumentada por el Comando Sur de las Fuerzas Armadas estadounidenses”.<sup>482</sup> Asimismo, se han realizado varios Simposios o Congresos (según la versión) sobre inteligencia regional, donde han asistido los Jefes de Inteligencia de la defensa de las Américas e invitados de otros países aliados (Europa). En Chile, el año 2011, fue sede de este encuentro, en 2012, en Brasilia, y en 2013, Guatemala.

Adicionalmente hay dos organismos multilaterales de inteligencia en los cuales participan países de Suramérica, se trata del Grupo de Acción Financiera Latinoamericana (GAFILAT) y la Oficina Regional de Enlace de Inteligencia (RILO). El propósito de GAFILAT, es

trabajar hacia el desarrollo y aplicación de una estrategia mundial integral para combatir el lavado de dinero y financiamiento del terrorismo .... El esfuerzo incluye alentar a la creación del delito de lavado de dinero en relación con delitos graves, el desarrollo de sistemas legales para investigar

y enjuiciar estos delitos, el establecimiento de sistemas para notificar las transacciones sospechosas, [y] la promoción de la asistencia judicial recíproca.<sup>483</sup>

Se orienta a fomentar la formación de las personas involucradas en los esfuerzos contra el lavado de dinero e identificar los factores regionales que deben tenerse en cuenta en la aplicación de las medidas contra el lavado de dinero. Los países Suramericanos miembros de GAFILAT son: Argentina, Bolivia, Brasil, Chile, Colombia, Ecuador, Paraguay, Perú, Uruguay.<sup>484</sup>

En el caso de RILO (Regional Intelligence Liaison Office) estamos ante

una red mundial para el intercambio de información entre las Aduanas de todo el mundo, que maneja datos relacionados con las actividades ilícitas relativas a materias aduaneras, y que opera bajo el marco de la OMA [Organización Mundial de Aduanas] (...) Esta red mundial de intercambio de información está apoyada por CEN [Customs Enforcement Network], que es un sistema de información que contiene datos acerca de las incautaciones de mercancías y actividades controladas por las aduanas de todo el mundo.<sup>485</sup>

En cada una de las regiones donde está RILO, existen puntos nacionales de contacto (NCP), que en el caso de los países de Suramérica corresponde a: Argentina, Brasil, Bolivia, Colombia, Ecuador, Guyana, Paraguay, Perú, Uruguay y Venezuela.

Un cuarto motivo, está dado por la experiencia en cooperación en inteligencia en organismos multilaterales de carácter geográficos como son el Mercado Común del Sur (MERCOSUR) y la Comunidad Andina de Naciones (CAN). En el caso de MERCOSUR, éste “se ha constituido un mecanismo institucionalizado de cooperación en seguridad pública e inteligencia criminal”<sup>486</sup> al nivel de que en diferentes

oportunidades y órganos de la RMI [Reunión de Ministros de Interior de MERCOSUR] se ha planteado la posibilidad relativa a la posible futura constitución de un órgano multinacional de análisis en inteligencia criminal (...), sin perjuicio de la existencia de mecanismos no formales, la

## Gestión de Inteligencia en las Américas

cooperación permanente e institucionalizada en materia de inteligencia en el MERCOSUR y MERCOSUR Ampliado ha estado limitada a la *inteligencia antiterrorista* y en menor grado, a otros aspectos de *inteligencia criminal*, no habiéndose llegado, aún en este último aspecto, a crear un ámbito permanentemente institucionalizado que comprendiera también a los aspectos fundamentales del *delito organizado*.<sup>487</sup>

En el caso de la CAN la cooperación en inteligencia “tuvo por característica, a diferencia de la que tiene lugar en el MERCOSUR, la confusión de los ámbitos de la seguridad pública y la defensa”.<sup>488</sup> Tal como lo explica Ugarte

la cooperación en inteligencia en el ámbito de la CAN fue organizada -fundamentalmente, ... en relación a determinados delitos – fundamentalmente narcotráfico, tráfico de armas- con participación de las fuerzas armadas en aspectos de seguridad interna y sin constituir ámbitos institucionales de cooperación en inteligencia (...) Con posterioridad, tal cooperación evolucionó hacia órganos de cooperación en inteligencia y en seguridad pública de alcance regional, carentes de institucionalización y de control político: CLACIP (Comunidad Latinoamericana y del Caribe de Inteligencia Policial) y AMERIPOL (Comunidad de Policías de América).<sup>489</sup>

Lo anteriormente indicado tiene ventajas y desventajas y no es el sentido en este trabajo hacer un juicio evaluativo al respecto, sólo nos limitamos a describir situaciones observadas.

En efecto, CLACIP-AMERIPOL

podría constituir una buena base para una cooperación institucionalizada en inteligencia criminal en la totalidad de los países Latinoamericanos y del Caribe – que, en caso de concretarse, resultaría de inestimable valor para la lucha contra el delito organizado. Para ello sería necesaria la firma de un tratado entre los respectivos países y la creación de órganos de administración y control, para lo cual EUROPOL -órgano al cual AMERIPOL, de algún modo, procuró imitar- podría constituir un buen modelo.<sup>490</sup>



Desde esta perspectiva, la posibilidad de cooperación en inteligencia resulta evidente pudiendo apreciarse una evolución en América Latina y el Caribe zonas geográficas que “han pasado de la casi exclusividad de la antigua cooperación hemisférica, a la creciente gravitación de las subregionales, y del predominio de la antigua cooperación fundada en el Conflicto Este – Oeste, al crecimiento de la cooperación en inteligencia basada en la seguridad pública”.<sup>491</sup>

El siguiente cuadro nos indica las posibilidades actuales de cooperación en inteligencia, en tres ámbitos. En el caso de la inteligencia militar y de la defensa, ésta puede concretarse en el ámbito del CDS en materia de: ataques cibernéticos a la defensa; ayuda ante situaciones de catástrofes y la protección de los recursos naturales, temas de interés según se ha establecido. Asimismo, refuerza la posibilidad de cooperación la indicación de intercambio de información en materias de defensa, para lo cual es condición necesaria, mas no suficiente que exista una coincidencia entre las políticas de seguridad y defensa de UNASUR – tal como es en el caso de la UE. También es posible desarrollar una base de datos común que alimentada con información que los países proporcionen, permita ser consultada por los países Suramericanos y que sea administrada por las direcciones de inteligencia de defensa en cada uno de los países de UNASUR, replicando así el modelo de SURNET, pero en este caso exclusivamente para UNASUR.

Tabla 14 Posibilidades de Cooperación en Inteligencia en UNASUR			
Posibilidades según Tratado Constitutivo de UNASUR	Tipo de Inteligencia		
	Inteligencia militar	Inteligencia policial y/o criminal	Inteligencia estratégica
q) la coordinación entre los organismos especializados de los Estados Miembros ...	X	X	X
s) el intercambio de información y de experiencias en materia de defensa	X		
t) la cooperación para el fortalecimiento de la seguridad ciudadana		X	

Tabla 14, (continua)			
Posibilidades de Cooperación en Inteligencia en UNASUR			
	Tipo de Inteligencia		
u) la cooperación sectorial como un mecanismo de profundización de la integración suramericana ...	X	X	X

**Fuente:** Elaboración de la autora, 2013.

En el caso de la cooperación en inteligencia militar, puede concretarse, por ejemplo, por medio de cursos comunes donde sea abordada la función inteligencia, lo cual puede hacerse en el curso de formación para civiles en defensa, como también, en el curso avanzado de política de defensa, que actualmente son impartidos en el marco del CDS. En estos cursos pueden incorporar tanto el tema de las actividades de inteligencia, como parte de los estudios de seguridad, como asimismo, la asignatura de inteligencia que permite conocer el modo en que funciona en cada uno de los países de UNASUR.

También, es posible enseñar técnicas comunes de análisis para identificar y prospectar temas de común interés, que en el marco de CDS, debiera estar asociado a amenazas externas comunes. En este sentido, la incorporación del tema de inteligencia como materia de estudio y en cursos de capacitación, se conversó en la reunión de Colombia en el 2012, en el encuentro de Ministros de Defensa de UNASUR.

En el caso de la inteligencia policial o criminal, la cooperación en UNASUR puede darse en el Consejo Suramericano en materia de Seguridad Ciudadana, Justicia y Coordinación de Acciones contra la Delincuencia Organizada Transnacional.<sup>492</sup>

Con relación a la inteligencia estratégica, la cooperación es posible concretarla por medio de encuentros de Jefes de Servicios de inteligencia. Éstos se reúnen para abordar temas solicitados por los Jefes de Estado, relacionados con dos tipos de materias: problemas específicos de países que afectan a otros países y es de interés conocer su impacto y anticipar posibles escenarios a enfrentar. Por cuanto, puede involucrar a varios países, por ejemplo, lo cual hace válida la extensión de cooperación en el ámbito multilateral.

Otra posibilidad para la cooperación en inteligencia es conocer el modo en que es entendido y prospectado por medio de escenarios situaciones que ocurren fuera del espacio geográfico de Suramérica, pero que puede afectarla seriamente. Por ejemplo, la crisis económica de la UE, la desaceleración del crecimiento chino, una guerra entre Corea del Norte y del Sur, la primavera árabe, un ciberataque a la infraestructura crítica de algún país suramericano o de un(os) país(es) fuera de esta zona geográfica con el cual hay una importante relación de intercambio de bienes y servicios entre otros.<sup>493</sup>

Una buena práctica observada en el caso de la UE puede ser replicada acá, se trata del EU IntCen instancia desde donde pueden ser monitoreados los eventos indicados, con participación de un grupo multidisciplinario de especialistas expertos (no funcionarios de los servicios de inteligencia) en las materias a las cuales se hace seguimiento. La finalidad de esta institución sería detectar anticipadamente posibles crisis regionales o fuera de la región para dar una alerta temprana de ello, generando así una capacidad preventiva que permita evitar la crisis o al menos una gestión beneficiosa del conflicto, desde la perspectiva de los intereses de los países de Suramérica.

Los informes que emita esta entidad pueden ser enviados a los encargados de inteligencia estratégica, policial y/o militar si hay materias de su interés. Cabe destacar la importancia que los temas abordados por esta entidad, haya sido previamente solicitado en la reunión de los Jefes de Estado de UNASUR, a quienes se les debe reportar periódicamente, independiente que en ocasiones se envíe copia a organismo especializado de UNASUR competente en la materia.

### Factores que limitan la cooperación internacional

Actualmente, “una cooperación institucionalizada en materia de inteligencia en los aspectos relativos a las relaciones internacionales, seguridad internacional y defensa, lucha hoy con la diversidad de intereses, la existencia de diversas concepciones de la seguridad y la defensa, y la persistencia de diferencias importantes pendientes en materia de política exterior, aunque nada pareciera insalvable en el mediano plazo”.<sup>494</sup> En este sentido, adquiere importancia identificar aquellos aspectos que limitan la cooperación en inteligencia con la finalidad de iniciar el camino hacia una institucionalización y estandarización de este proceso.

Para referirnos a esta materia, será considerada la cooperación en inteligencia en forma genérica y no según los ámbitos de aplicación. No obstante, se

## Gestión de Inteligencia en las Américas

menciona algún aspecto específico en cada ámbito, sólo en caso que sea de particular relevancia al argumento planteado.

La primera limitación a identificar para cooperar en inteligencia, está relacionada con la inexistencia en algunos países de organismos de inteligencia homólogos para relacionarse entre instituciones similares de los diferentes países. En efecto, la carencia de interlocutores válidos para comunicarse, entregar y/o solicitar datos, información y/o inteligencia, como asimismo, realizar una actividad de investigación y/o análisis u operativa conjunta impide el eficaz intercambio de información.

Actualmente, la mayoría de los países de UNASUR cuenta con organismos de inteligencia en el ámbito estratégico, militar y policial. Aunque hay países que no cuentan con organismos en alguno de estos ámbitos, ello no implica que la actividad no se realice. Sin embargo, en tales casos, para efectos de cooperación ésta se encuentra prácticamente imposibilitada de realizarse. La disponibilidad de instancias de cooperación genera incentivos para los países que no cuentan con estos organismos para crearlos y así acceder a una fuente de información disponible.

Desde una perspectiva cultural, es necesario que cada país cuente con capacidad para confirmar la validez de la información recibida y que ésta sea una exclusiva fuente de información, por cuanto, si la información entregada es equivocada generará una profunda desconfianza que limitará la posterior cooperación, no sólo por haber recibido información equivocada, sino también por los daños eventuales que pueda generar el análisis basado en la información incorrecta.

En este sentido, se reconoce que la información obtenida a través de la cooperación en inteligencia, no supe las capacidades propias para generar los datos o información y generar inteligencia propia que permitirá satisfacer las necesidades del consumidor (autoridad política para su proceso decisional). Son las limitadas capacidades del propio servicio las que justifica la cooperación en inteligencia, pues podrá accederse a información que adicionada a la obtenida permitirá confirmar o descartar hipótesis o escenarios con respecto a determinados fenómenos.<sup>495</sup>

Asimismo, “el tradicional enfoque de otro país y de sus capacidades de inteligencia como un enemigo probable -aun cuando pueda ser aliado- dificulta

la cooperación”.<sup>496</sup> Ello es particularmente relevante, en la zona geográfica de UNASUR, por cuanto, entre varios países de Suramérica han existido serios conflictos de seguridad. No obstante, el reconocimiento de que “hay siempre más información potencialmente disponible que lo que una agencia puede recolectar por sí misma”, junto al hecho de que “la globalización ha sido crucial para reconfigurar el crimen organizado dentro de un contexto nuevo y claramente transnacional”<sup>497</sup> y con ello generar problemas que afectan la seguridad internacional de los países a partir de la existencia de amenazas transnacionales, ha producido esta urgente necesidad de potenciar la cooperación en inteligencia. Sin embargo, la identificación de amenazas comunes es solamente el primer paso hacia cooperación en inteligencia, y en este sentido, podemos señalar que constituye una condición necesaria más no suficiente para su logro.

Profundizar en el proceso de cooperación en inteligencia hasta llegar a la institucionalización, estará condicionado por la posibilidad de avanzar en la trilogía conocimiento – confianza – cooperación. Considerando que la etapa final de la cooperación en inteligencia, después de “conocimiento, confianza, y cooperación”, puede ser institucionalizarla, “estudios en el campo de la cooperación policiaca internacional muestran que la informalidad es un prerrequisito de la confianza: sin la consolidación de una red informal, la cooperación policiaca no prosperará”.<sup>498</sup> En el caso de todos los países Suramericanos, hemos observado que existe en mayor o menor medida cooperación en inteligencia, de índole policial tanto como militar. Pero sus características se asemejan a una cooperación no institucionalizada (por no estar respaldada por un tratado firmado por el Presidente de la República, ratificada en el Congreso Nacional y sujeto a controles que van más allá de los organismos que realizan la cooperación).<sup>499</sup>

En efecto, si existe un alto nivel de corrupción en el país y/o percepción del mismo en relación a los servicios de inteligencia, especialmente en la opinión de otros servicios de inteligencia nacionales, la cooperación internacional en inteligencia será mínima o nula, por cuanto, la confianza no logra establecerse. Lo mismo ocurre cuando existe una alta rotación de funcionarios en los servicios de inteligencia, que se asocia con la falta de profesionalismo. En el caso de los países de UNASUR, estas situaciones han ocurrido, y aunque ello no ha sido periódico ha dañado seriamente la confianza en el servicio, y con ello las oportunidades de cooperación en inteligencia no son frecuentes.<sup>500</sup>

### Consolidando las ventajas de cooperación en inteligencia

Profundizar en la cooperación requiere transitar la cooperación informal hacia un estado más formal, es decir, tender hacia la institucionalización de sus procesos, lo cual ofrece ventajas como por ejemplo, al otorgar mayores niveles de seguridad en el intercambio de información. Otra ventaja puede emerger de una mejor calidad de la formación profesional de los funcionarios, debido a un proceso de entrenamiento o educación formal que puede extenderse a todo el personal de los servicios de inteligencia, generando así un perfil más profesional y elevando la confianza de las diferentes agencias de los países de la zona suramericana. A la vez, hay que tener presente la posibilidad que las iniciativas basadas en relaciones informales no sean suprimidas por la misma institucionalización, es decir, la formalización de las relaciones y procesos no suple a la relación de información, sino que lo complementa y profundiza.

En este sentido, “el establecimiento de un mecanismo de cooperación formal con vocación de permanencia, además de suponer un mínimo de instrumentación de carácter secreto, suele suponer reuniones periódicas entre los participantes, personal de enlace, estándares comunes de clasificación, y medidas de seguridad de contra inteligencia equivalentes”.<sup>501</sup> En esta perspectiva, la inexistencia de lo anteriormente descrito, genera una situación de cooperación en inteligencia limitada en UNASUR, resultado de acuerdos de intercambio de información separados que no se da en el marco de esta asociación sino que como resultado de diversos convenios en los que participan los países que forman parte de Suramérica.

En síntesis, los países de UNASUR no tienen acuerdos de cooperación en inteligencia, aunque el tema ha sido profusamente mencionado en varias reuniones, el tema no está incorporado a la agenda. No obstante, los países que componen UNASUR cuentan con organismos de inteligencia y poseen experiencia de cooperación en inteligencia en el marco de otras instancias internacionales multilaterales. Avanzar en la ampliación de esta cooperación (que abarque a todos los países de UNASUR) y profundización de ésta requiere la superación de una serie de limitaciones que hoy existen entre la que destaca la necesidad de homogeneizar y hacer coincidentes la política exterior y de defensa de los países de UNASUR, tarea hoy pendiente pero que va en ese camino.

## Conclusiones

Son identificados al menos cuatro motivos que justifican la promoción de la cooperación en inteligencia en el marco de UNASUR. El primero referido a la constatación de amenazas comunes, establecidas en el Tratado Constitutivo de UNASUR. Asimismo, un segundo motivo se relaciona con la existencia mayoritaria en los países Suramericanos de una capacidad en inteligencia policial, militar y estratégica. Un tercer motivo considera la experiencia de éstos -aunque principalmente informal- de cooperación en inteligencia en organismos temáticos multilaterales de cooperación en inteligencia (por ejemplo, RILO, GAFI, CLACIP). Finalmente, un cuarto motivo se encuentra en la experiencia de cooperación en inteligencia – orientado fundamentalmente a la seguridad pública y ciudadana, observada en organismos multilaterales como MERCOSUR y CAN. Ello permite justificar la afirmación que los países de Suramérica pueden avanzar hacia una cooperación más formal en inteligencia en el marco de UNASUR.

Según lo revisado, no existen acuerdos de cooperación en inteligencia firmados en UNASUR por parte de las más altas autoridades de este organismo multilateral Suramericano. No obstante, existe una informal cooperación en inteligencia entre los países Suramericanos.

Esta cooperación informal es resultado de diversos convenios firmados entre organizaciones homólogas de inteligencia en el marco de instancias multilaterales diferentes de UNASUR, que sin embargo, considera a muchos de estos países. Es el caso en el ámbito policial de CLACIP realizado en el marco Latinoamericano y del Caribe; en el ámbito de la inteligencia estratégica, a través del foro Iberoamericano de Directores de Servicios de Inteligencia y; en el ámbito de la inteligencia militar, mediante la base de datos en red SURNET administrada por las direcciones inteligencia de defensa de países americanos organizado a instancia del Comando Sur de EE.UU.

La experiencia de la UE en este sentido puede ilustrar las posibilidades, constatándose la pertinencia y necesidad para el caso de UNASUR de contar con un Centro de Situación (SitCen), que asesore a los más altas autoridades nacionales y de UNASUR y realice la fusión de la inteligencia estratégica, militar y policial para identificar escenarios que afecten la seguridad de los países Suramericanos, como también, en lugares geográficos donde los países

## Gestión de Inteligencia en las Américas

de UNASUR tengan intereses estratégicos. Asimismo, este SitCen, puede ser una útil herramienta en la prevención de crisis y manejo de conflictos que afecten conjuntamente a los países de UNASUR.

Asimismo, la realización de cursos en temas relacionados con la seguridad de los países y las amenazas que ellos enfrentan en el marco de UNASUR ofrece una oportunidad para estandarizar la formación en materia de inteligencia, avanzando de este modo en una homologación del lenguaje y las técnicas de análisis en el tema, abriendo la oportunidad para futuras investigaciones y operaciones conjuntas, por ejemplo, en temas relacionadas con el delito y/o crimen organizado.

Finalmente la elaboración de bases de datos interoperables permitirían el intercambio de información en tiempo real entre los países que forman parte de UNASUR en los temas que han declarado de común preocupación. Lo anterior sólo puede concretarse si es posible avanzar en la trilogía “conocimiento – confianza – cooperación”, que en materia de inteligencia en UNASUR se encuentra entre la etapa 1 y 2 de la trilogía. En este sentido, la principal limitación al progresar en la cooperación está dado por la falta de confianza, en las personas y sus instituciones, reflejado muchas veces en escándalos en los servicios de inteligencia, la alta rotación de sus funcionarios y la salida de algunos de ellos quienes han llegado a la cárcel inclusive, impidiendo de este modo la generación de confianza mínima para lograr la cooperación.

Cabe destacar la relación entre cooperación información y formal, en términos que son complementarias y no es deseable la sustitución de una por la otra. En efecto, acuerdos de cooperación que traten de limitar el contacto informal entre los servicios y sus funcionarios, traerán como consecuencia la limitación a la cooperación, pues el mecanismo de coordinación entre ambos servicios se verá afectado.

Al concluir, es importante señalar que la existencia de un estado informal de cooperación en inteligencia, no constituye una situación negativa, al contrario puede ser considerado como un positivo primer paso en el que es necesario avanzar por parte de los gobiernos de los países de Suramérica, como también, las altas autoridades de UNASUR. En los dos ámbitos, se puede acelerar este proceso colocando el tema de la inteligencia en la agenda de temas a considerar en sus reuniones. Al respecto se han observado tímidas



iniciativas que no han logrado prosperar, quedando en evidencia que es necesario un mayor liderazgo en el tema.

### Biografía de la autora

**Carolina Sancho Hirane** se ha desempeñado como Jefa del Departamento de Crimen Organizado del Ministerio del Interior y Seguridad Pública, también ha sido Jefa de la Cátedra de Inteligencia en la Academia Nacional de Estudios Políticos y Estratégicos (ANEPE) de Chile donde imparte docencia en materia de inteligencia a nivel pre grado, post grado y postítulo. Asimismo, ha sido profesora en la Escuela de Gobierno y Gestión Pública de la Universidad de Chile con la asignatura “Análisis de Conflictos Internacionales actuales”, en la Universidad de Santiago de Chile ha impartido la asignatura de "Construcción de Procesos de Paz" en la licenciatura de Relaciones Internacionales y en la Academia de Guerra Aérea la asignatura de “Inteligencia”, entre otras instituciones académicas. Tiene Título Profesional de Administrador Público de la Escuela de Gobierno, Gestión Pública Ciencia Política, y Magíster en Ciencia Política, Instituto de Asuntos Públicos, Universidad de Chile. Está doctoranda en la Universidad de Zaragoza (España). Correo: csanchohirane@yahoo.es.

### Sección III

## Gestión de la Privacidad vs. Seguridad y Comunidades de Inteligencia



## Gestión de la Privacidad vs. Seguridad y Comunidades de Inteligencia

José Manuel Ugarte

*Hay entre aquellos empleados en la comunidad de inteligencia y seguridad de nuestro país... quienes sienten que tienen una licencia para operar libremente fuera de los dictados de la ley e incluso para actuar como lo creen oportuno. Los funcionarios públicos de cualquier nivel, cualquiera sea su posición, como cualquier otra persona, deben respetar y honrar las leyes de los Estados Unidos.*

—Juez Barrington Parker<sup>502</sup>

### Derechos individuales, privacidad y actividad de inteligencia

El tema de esta sección impone una descripción de los desafíos que plantean determinadas características de la actividad de inteligencia para la privacidad de los habitantes y de los procedimientos establecidos para la protección de dicha privacidad. La actividad de inteligencia, por sus características, puede entrar en colisión con los derechos individuales. Ese conflicto no tiene la misma solución en un Estado democrático, que en un Estado totalitario; tal como la referida actividad no tiene características similares en uno y otro caso.<sup>503</sup>

Como hemos señalado en otras oportunidades,<sup>504</sup> la actividad de inteligencia posee características -como el secreto que protege identidades, fuentes, métodos y operaciones- que contradicen principios fundamentales del Estado democrático, como la publicidad de los actos de gobierno. También emplea un instrumental concebido para la penetración de la privacidad.

Esta contradicción entre una característica fundamental del sistema republicano y un aspecto de la actividad de inteligencia es salvada a través de los *límites y el control*. De ello se deriva que en un Estado democrático, la actividad de inteligencia debe ser esencialmente, limitada, particularmente en lo que se refiere al interior del país.

En dicho ámbito, entendemos que el objeto de la actividad de inteligencia -incluyendo a la *contrainteligencia*- debe estar constituido por las concretas amenazas a la seguridad del Estado, provocadas por actividades dirigidas contra él por países extranjeros, o por organizaciones extranjeras o nativas que

procuren atentar contra el Estado, cambiar por medios ilegales su sistema de gobierno, o atentar contra las autoridades del país o el legítimo ejercicio por parte de éstas de sus atribuciones.

En el exterior del Estado, la actividad de inteligencia debe estar dirigida a prevenir o conjurar amenazas contra la seguridad del Estado, incluyendo las que tengan por objeto la seguridad de los países aliados; y a promover intereses nacionales, particularmente en materia de política exterior, defensa, o economía.

El control de los órganos y actividades de inteligencia debe ser aceptado y asumido como una consecuencia del carácter republicano y democrático del Estado, y la exigencia de legitimidad y de eficacia que dicho carácter plantea para toda institución gubernamental. Consideramos adecuado destacar que en un sistema democrático plenamente vigente, no debería existir contradicción entre la protección de la privacidad por una parte, y la seguridad y las comunidades de inteligencia por otra. Ello así, porque el profesional de inteligencia de un Estado de tales características sabe que la vigencia de los derechos individuales forma parte del Estado que debe defender a través de su actividad.

Un aspecto de los límites y de los controles, es la protección de la privacidad. Reconocida en los textos constitucionales de la generalidad de los Estados Americanos, habremos de recordar aquí que en América, la Convención Americana de Derechos Humanos<sup>505</sup> (artículo 11) estableció el “derecho de toda persona ... al respeto de su honra y al reconocimiento de su dignidad” como la prohibición contra “injerencias arbitrarias o abusivas en la vida privada de las personas, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación”, como al “derecho a la protección de la ley contra esas injerencias o esos ataques”.

Habremos de referirnos aquí a los instrumentos establecidos en la legislación destinados a su protección, sin dejar de reconocer la importante contribución que hacen al fin indicado la existencia de adecuados controles de la actividad de inteligencia, así como la estricta delimitación de las competencias en materia de inteligencia interior.<sup>506</sup>

### Los instrumentos específicos de protección de la privacidad

Constituyen medios de protección de la privacidad respecto de la actividad de inteligencia, los requisitos autorizatorios para el empleo por parte

## Gestión de Inteligencia en las Américas

de tal actividad, dentro del propio país, de medios y procedimientos de interceptación de comunicaciones telefónicas, telegáficas, por facsímil, o de transmisión de voces, paquetes de datos u objetos a distancia, incluyendo la interceptación de la correspondencia y del correo electrónico. También, para la captación electrónica de conversaciones privadas, el ingreso en domicilios privados, el seguimiento y otras formas de vigilancia.

Estos requisitos autorizatorios son de otorgamiento judicial en diversos países, tales como los países americanos, España y Unión Sud-Africana, constituyendo parte del control judicial de la actividad de inteligencia, integrado también por aspectos como control de protección del derecho de acceso a la información, protección de datos personales, y de trasgresiones a la ley realizadas con motivo de la actividad de inteligencia – mientras en la mayoría de los países europeos, el otorgamiento de la autorización está a cargo de ministros del órgano ejecutivo, generalmente con controles posteriores.

Los controles de medidas intrusivas de la privacidad tienen por finalidad verificar que estas acciones tengan por finalidad aquellas invocadas para su realización, y que la intrusión en la privacidad quede reducida al mínimo posible.<sup>507</sup> Entre aquellos países en los cuales existe el control judicial de actos intrusivos de la privacidad pueden advertirse dos modalidades diversas. La primera, es la que establece que el control sea realizado por jueces y tribunales ordinarios -tal como se efectúa en Canadá y en Argentina- y la segunda, es la realización de dicho control por un tribunal especial, bien que constituido por magistrados judiciales, como sucede con el tribunal previsto en el Título 50, Capítulo 36, Subcapítulo I, apartado 1803 del Código de Estados Unidos para expedir autorizaciones de vigilancia electrónica para propósitos de inteligencia—*Foreign Intelligence Surveillance Act* (FISA).

En este último supuesto, interviene un tribunal conformado a través de la elección por el Presidente de la Corte Suprema estadounidense de once jueces de corte de distrito de siete de los circuitos judiciales, que constituyen un tribunal con jurisdicción relativa a solicitudes para realizar vigilancia electrónica dentro del territorio de Estados Unidos, existiendo también un tribunal de revisión constituido por tres jueces de los tribunales de apelación de distrito designados del mismo modo.

Las leyes sobre inteligencia pueden limitarse a prever las interceptaciones de comunicaciones, como sucede con la Ley N° 25520 argentina -no

contemplando otros medios intrusivos de la privacidad- mientras que leyes de otros países prevén bajo el rótulo “procedimientos especiales de obtención de información” detallándolos, como la Ley N° 19974<sup>508</sup> chilena no sólo la interceptación de comunicaciones de todo tipo -incluyendo las postales- sino también la escucha y grabación electrónica incluyendo la audiovisual, previéndose además la facultad para los jefes de los organismos de inteligencia de utilizar sin autorización judicial informantes e incluso la facultad otorgada a los jefes de organismos policiales y militares sin autorización judicial, de utilizar como agentes encubiertos a funcionarios que se introduzcan en organizaciones sospechosas de actividades criminales, dentro de las competencias de su servicio y limitados al resguardo de la seguridad nacional de Chile y a su protección de las amenazas del terrorismo, narcotráfico y delito organizado.

La Ley del Servicio Canadiense de Inteligencia de Seguridad establece con detalle las actividades sujetas a autorización judicial, incluyendo, además de la interceptación de comunicaciones, obtener cualquier información, registro, documento o cosa y con tal finalidad, a entrar en cualquier lugar, obtener acceso a alguna cosa, buscar, remover, examinar, tomar extractos de, hacer copias de, o registrar de cualquier otra manera, o instalar, mantener o remover algún cosa, cubriendo en definitiva virtualmente todas las posibilidades de acción intrusiva.<sup>509</sup>

Con relación a la ejecución de la medida, en lo que a interceptación de comunicaciones se refiere, existen supuestos que confían la ejecución de la medida al propio organismo de inteligencia, como sucede con la Ley N° 25520 argentina, o bien otros como la Ley N° 19974 chilena, que dispone que las interceptaciones de comunicaciones solicitadas por la Agencia Nacional de Inteligencia -ANI- deben ser ejecutados por la Fuerza del Orden y Seguridad que se indique en la resolución respectiva, quien debe dar cuenta al Director de la ANI de la operación y de sus resultados.<sup>510</sup>

Finalmente, existen en Latinoamérica leyes orgánicas sobre inteligencia o de establecimiento de controles sobre aquélla que no comprenden disposiciones relativas a protección de la privacidad que pueden hallarse en otras leyes, como la Ley N° 9883 brasileña. También la Ley Estatutaria N° 195/2011 de Colombia participa de esa característica<sup>511</sup> así como la Ley N° 750 de Seguridad Democrática de Nicaragua<sup>512</sup> o la Ley Marco del Sistema Nacional de Seguridad de Guatemala.<sup>513</sup>

## Gestión de Inteligencia en las Américas

Con relación al caso brasileño, cabe destacar la presencia en la Constitución de 1988, de una disposición que garantiza la inviolabilidad de las comunicaciones, salvo orden judicial que puede emitirse exclusivamente para fines de investigación criminal o instrucción procesal penal, aspecto reglamentado por la Ley N° 9296 (1996) limitando la interceptación de comunicaciones a la investigación de delitos serios, y asignando la ejecución de la medida exclusivamente a la policía. Como puede verse, la interceptación de comunicaciones para inteligencia quedó excluida del orden jurídico brasileño.

En materia de protección de la privacidad, otro medio de importancia es la protección de datos personales, respecto de la actividad de inteligencia. En Latinoamérica, las leyes orgánicas en materia de inteligencia no contienen referencias a la protección de datos personales respecto de tal actividad, -bien que la generalidad de los países de la región poseen normas legales e incluso constitucionales sobre la materia- con la única excepción de la Ley Estatutaria 195/2011 colombiana, que posee disposiciones de eficacia limitada, por hallarse su cumplimiento bajo control prácticamente exclusivo del órgano ejecutivo, no previéndose posibilidades de acceso y de rectificación, actualización, o supresión por parte de los habitantes. Se trata de una protección débil, si se la compara con casos extrarregionales como la Ley de los Servicios de Inteligencia y Seguridad de 2002 del Reino de Holanda.<sup>514</sup>

### Comentarios a los artículos integrantes de esta sección

#### *Profesora Dra. Priscila Brandão*

El artículo de Priscila Carlos Brandão nos proporciona un análisis de la problemática del Sistema de Inteligencia Brasileño (SISBIN) y dentro de él, del Subsistema de Inteligencia para la Seguridad Pública (SISP).

Además de analizar el nacimiento, la evolución y las dificultades experimentadas por el SISP, y, en general, por la inteligencia criminal brasileña, el artículo presenta una realidad que es común a otros países latinoamericanos: la subsistencia en diversos países de la región, tras el Conflicto Este-Oeste, de modelos de inteligencia caracterizados por un organismo de inteligencia civil con muy amplias competencias en materia de inteligencia no sólo en el área exterior y en contrainteligencia, sino también en inteligencia interna a la nación. En el caso brasileño, la competencia de la ABIN comprende,



“la producción de conocimientos destinados a asesorar al Presidente de la República”<sup>515</sup> siendo “agencia central” del SISBIN. Asimismo, el SISBIN incluye también a la inteligencia criminal, bajo el nombre de “inteligencia de seguridad pública”. También refiere Priscila Carlos Brandão otro problema muy frecuente en Latinoamérica, cual es la persistencia tras el Conflicto Este-Oeste -con conceptos doctrinarios similares a los entonces vigentes- de organismos de inteligencia militares que incluyen en sus competencias la seguridad interior. Frente a esa realidad, también se fue produciendo en Brasil -y en la región- ante el desafío representado por el delito organizado, el surgimiento de la inteligencia criminal<sup>516</sup> frente a la tendencia de organismos de inteligencia civiles y militares de incursionar en esa temática.

Esto explica que al constituirse el SISP, haya sido la ABIN -pese a su condición de organismo de inteligencia gubernamental o de Estado- designada “agencia central”, con preferencia a los órganos específicos del área- y que aún al enmendarse ello con la designación como “agencia central” a la Secretaría Nacional de Seguridad Pública (SENASP-MJ), el SISP estuviera constituido predominantemente por organismos estrictamente ajenos al área. También, que al crearse el Consejo Especial del SISP (CE-SISP) destinado a establecer normas para las actividades de inteligencia para la seguridad pública, bajo la presidencia del Secretario Nacional de Seguridad Pública (SENASP), igualmente el predominio fuera para representantes de organismos no pertenecientes estrictamente al ámbito de inteligencia criminal,<sup>517</sup> mientras que los órganos de inteligencia de seguridad pública de los Estados y del Distrito Federal, lo integraran sólo como miembros eventuales, sin derecho a voto.<sup>518</sup>

Otras peculiaridades señaladas por Priscila Brandão: la debilidad, en términos de medios humanos y materiales, de la Coordinación General de Inteligencia (CGI) y consiguiente dificultad para desempeñar las importantes funciones que como agencia central del SISP le asignara la Resolución N° 1/2009 de la SENASP-MJ, en materia de orientación y supervisión del SISP; la orfandad normativa en que se desenvuelve la actividad de inteligencia de seguridad pública, y el fracaso de las gestiones tendientes a la presentación y tramitación de un proyecto de ley sobre inteligencia de seguridad pública; la oposición por parte de la ABIN y las fuerzas armadas al dictado de una Doctrina de Inteligencia de Seguridad Pública -bien que ésta fuera finalmente aprobada- no constituyen a nuestro criterio sino consecuencias del mismo fenómeno, por

## Gestión de Inteligencia en las Américas

cierto no exclusivamente brasileño, sino, en buena parte, común a Latinoamérica: la puja, por parte de los organismos de inteligencia civiles e incluso en algunos países de los militares, por retener e incluso incrementar su participación en materia de delito organizado, frente al paulatino desarrollo, en América Latina, de la inteligencia criminal, a cargo de las policías y también, en Argentina y Guatemala, de organismos de inteligencia criminal. En la Argentina, este organismo es la Dirección Nacional de Inteligencia Criminal de la Policía Federal y en Guatemala es la Dirección General de Inteligencia Civil (DIGICI) del Ministerio de Gobernación.<sup>519</sup>

Debe también computarse dentro del fenómeno descrito, que la Doctrina de Inteligencia para la Seguridad Pública (DNISP) brasileña de 2009, verdadero logro del país (única en Latinoamérica) esté basada, en realidad, en los procedimientos correspondientes a la inteligencia de Estado o gubernamental, propia de la ABIN.<sup>520</sup>

Creemos que lo que incide en las características y desempeño del SISP brasileño es su ya señalada composición, en la que los participantes del ámbito de la inteligencia criminal constituyen una minoría. Ello se refleja con toda claridad en el artículo 7° de la reglamentación del SISP aprobada por la Resolución N° 1/2009 de la SENASP-MJ, donde se establece que su actividad tiene como “foco principal”, la seguridad pública, entendida éste como delito organizado y otras formas de delitos graves y de gran repercusión social, pero también como “foco secundario ... hechos relativos a la dinámica social que puedan atentar contra la seguridad interna” e incluso un “foco político e administrativo”, con “hechos relativos a la demanda social”. Esto pertenece, en el mejor de los casos, al mundo de la inteligencia de seguridad y no a la seguridad pública.

En nuestra opinión, la solución de la cuestión no pasa por la autonomía de la inteligencia policial ni por conferir carácter informal al intercambio de información en materia de inteligencia criminal, sin dejar de reconocer los hallazgos de Michael D. Bayer en *The Blue Planet*.<sup>521</sup> Aunque es exacto que el intercambio informal de informaciones entre funcionarios policiales basado en el conocimiento y la confianza personal constituye un poderoso auxiliar para la investigación de los delitos, y que por ello es útil, no creemos que pueda constituir la regla, menos aún entre participantes de distintos países. Consideramos que en cuestiones en las que están en juego la libertad de las

personas, los ámbitos de cooperación bajo control de los Estados respectivos o de organismos internacionales formalmente constituidos -tales como EUROPOL en el ámbito europeo, o INTERPOL en el ámbito internacional, o los ámbitos de cooperación construidos en los procesos de integración latino-americanos-<sup>522</sup> debe constituir la regla.

Lo que en realidad cabe extraer del inusualmente rico artículo de Priscila Brandão, es que los problemas puestos de manifiesto por la autora vienen en buena medida de la utilización en materia de inteligencia criminal de métodos, procedimientos y normas (incluyendo el uso excesivo de la clasificación) propios de la inteligencia gubernamental o de Estado, pero inadecuados para la inteligencia criminal.

Es que existe una verdadera diferencia de naturaleza entre la inteligencia criminal, por una parte, y la inteligencia de Estado y la inteligencia militar, por la otra. La inteligencia criminal es la aplicación de la metodología propia de la actividad de inteligencia, especialmente en materia de análisis, a la actividad policial y de seguridad pública.<sup>523</sup> Se ha definido a la “inteligencia criminal como ... la creación de un producto de conocimiento de inteligencia que apoya la toma de decisiones en las áreas de accionar policial, reducción del delito, y prevención del delito”.<sup>524</sup>

Por esa razón, en aquellos países en los cuales la inteligencia criminal ha tenido mayor desarrollo -muy especialmente el Reino Unido, Canadá, Australia, Italia, la República Federal de Alemania- la inteligencia criminal se rige por leyes diversas a la actividad de inteligencia en sentido estricto; no integra los sistemas de inteligencia nacionales -aunque, obviamente, existan vasos comunicantes- y posee normas y procedimientos diversos. Totalmente a diferencia de Latinoamérica, donde se rige por las mismas normas propias de la actividad de inteligencia e integra los sistemas de inteligencia nacionales, careciendo de una doctrina propia, excepción hecha de Brasil en que, como se ha visto, la doctrina vigente reconoce una fuerte influencia de la inteligencia de Estado. La característica latinoamericana de incluir a los órganos de inteligencia policial y a los organismos de inteligencia criminal como miembros plenos de sus sistemas de inteligencia, sujetándolos a las mismas normas vigentes para los organismos de inteligencia *strictu sensu*, no está presente en los países de mayor desarrollo institucional en la materia, que con contadas

## Gestión de Inteligencia en las Américas

excepciones, han sabido mantener una distinción entre la actividad de inteligencia y la actividad policial.

Creemos que la solución de los problemas planteados en Brasil por Priscila Brandão -pero vigentes en Latinoamérica- se encuentra en una ley sobre inteligencia criminal, que norme todos los aspectos de esta actividad con criterios propios de ésta; y una doctrina de inteligencia criminal que, como lo hace el Modelo Nacional de Inteligencia inglés (NIM) elaborado en base a la iniciativa de la Asociación de Jefes de Policía de Inglaterra y Gales y el liderazgo del entonces Servicio Nacional de Inteligencia Criminal inglés,<sup>525</sup> esté elaborada específicamente para la actividad policial y de seguridad pública.

Lejos de estimular la compartimentación y la excesiva clasificación, el NIM estimula el intercambio de información entre las instituciones policiales participantes, a través de la actuación en tres niveles -local, regional y nacional-internacional-, la elaboración de productos de inteligencia estandarizados, para facilitar su intercambio y utilización, promoviendo la organización y la adecuada utilización del conocimiento, sistematizando las normas y procedimientos de actuación entre los participantes.

El éxito del Modelo ha dado lugar a la conformación, en EUROPOL, de un Modelo Europeo de Inteligencia elaborado siguiendo su orientación.<sup>526</sup>

### *Mag. Liza Zúñiga Collado*

Liza Zúñiga Collado plantea en su artículo temas entre los que destacan la conveniencia y necesidad de la creación y funcionamiento de un órgano de inteligencia en el ámbito penitenciario, y un análisis de la instrumentación legislativa de la actividad de inteligencia en América Latina.

Chile -como sucede en la gran mayoría de los países del mundo, inclusive latinoamericanos- cuenta ya con un órgano de inteligencia dentro de Gendarmería de Chile, institución que en ese país tiene a su cargo la función de vigilancia y contribución a la reinserción de las personas privadas de libertad.<sup>527</sup> Se trata del Departamento de Investigación y Análisis Penitenciario, cuya misión consiste en “estudiar y analizar información relevante en materia de seguridad penitenciaria” hallándose entre sus funciones, la de “Recolectar y

procesar información relativa a la seguridad penitenciaria con el objeto de asesorar a la autoridad institucional en la toma de decisiones”.<sup>528</sup>

En Chile se ha integrado la inteligencia penitenciaria a la inteligencia criminal. En efecto; en Chile, a poco de creado el Ministerio del Interior y de Seguridad Pública en 2011, tuvo lugar la creación del Centro Estratégico de Análisis del Delito (CEAD).<sup>529</sup> Se trata de un órgano de inteligencia criminal<sup>530</sup> (análisis del delito)<sup>531</sup> a partir de información generada por las instituciones protagonistas del sistema penal: Gendarmería de Chile, Carabineros de Chile, Policía de Investigaciones, Poder Judicial y Ministerio Público, quienes suministran información delictual a través de la Plataforma Integrada de Servicios Electrónicos del Estado, conformándose un Sistema Unificado de Datos Criminales, un Observatorio Nacional de Seguridad Pública y, fundamentalmente, una Sala de Análisis del Delito, que integran analistas del Ministerio del Interior y Seguridad Pública, de Gendarmería de Chile, de Carabineros de Chile y de Policía de Investigaciones. De particular interés resulta la Sala de Análisis del delito, a través de la cual, realizándose análisis espacial, temporal, personal, ambiental, y de *modus operandi* del delito, se pretende obtener con el auxilio de herramientas informáticas patrones y tendencias delictivas, destinadas a facilitar la prevención y represión del delito.

Cabe señalar que, de modo de facilitar el trabajo de la Sala de Análisis del Delito, en fecha reciente -19 de diciembre de 2012- se ha procedido a la firma en Chile, del acuerdo entre representantes del Poder Judicial, Ministerio Público, Ministerio de Justicia, Gendarmería de Chile, Carabineros de Chile, Policía de Investigaciones, Servicio Nacional de Menores y Servicio de Registro Civil e Identificación, de creación del Banco Unificado de Datos Criminales (BUD).

Como puede advertirse, en Chile, el servicio penitenciario no sólo aporta información sino también sus propios analistas, participando de modo integral en el suministro de información criminal y en su análisis.

Algo similar sucede en Argentina, donde también el Servicio Penitenciario Federal cuenta con un órgano de inteligencia, el Departamento de Inteligencia Penitenciaria, que suministra información a la Dirección Nacional de Inteligencia Criminal, organismo de inteligencia al cual la Ley N° 25520 de Inteligencia Nacional asigna la función relativa a la producción de inteligencia criminal (art. 9). En la medida en que se percibe una aproximación similar por

## Gestión de Inteligencia en las Américas

parte de otros países de la región, se puede concluir aquí que la inteligencia penitenciaria constituye un importante auxiliar de la lucha contra el delito.

Cierto es que en las leyes de inteligencia de los países latinoamericanos no figuran tales órganos de inteligencia...como tampoco lo hacen, en la generalidad de las leyes de inteligencia de otras regiones del mundo.<sup>532</sup> Lo que sucede es que el aporte de la inteligencia penitenciaria es, fundamentalmente, a la inteligencia criminal, a la lucha contra el delito, no a la inteligencia estratégica nacional o de Estado. Por otra parte, la misión fundamental de las instituciones penitenciarias es el cumplimiento de las penas privativas de libertad y la resocialización de los internos, no la inteligencia estratégica; lo que no significa negar la importancia que tiene la inteligencia penitenciaria para la prevención y represión del delito, ni la necesidad de asegurarle adecuados canales de comunicación con oficiales representativos de la inteligencia nacional o estratégica, idealmente a través de la inteligencia criminal.

Como es sugerido en el trabajo de Liza Zúñiga Collado, la actividad legislativa con relación a la inteligencia en América Latina es uno de los fenómenos más llamativos dentro del ámbito de la defensa nacional y seguridad interior latinoamericanos en los últimos años, más allá de que en muchos casos haya limitaciones y defectos y, por sobre todo, que sea preciso avanzar desde las reformas formales hacia las reformas reales.<sup>533</sup>

### *Dr. Russell Swenson y Mag. Zulia Yanzadig Orozco Reynoso*

En este trabajo se abordan aspectos relativos a la cooperación internacional y la coordinación nacional en la actividad de inteligencia, y su incidencia en la vigencia de los derechos individuales y en la eficiencia y eficacia en dicha actividad.

Ello, a partir del análisis de un artículo de Elizabeth Sepper<sup>534</sup> en el que se alerta sobre las negativas consecuencias, para la vigencia de los derechos humanos -y en general, para la legitimidad y eficacia de la actividad de inteligencia- que se derivarían del carácter discrecional y no sujeto a controles del intercambio internacional de inteligencia. Se nota el auge de dicho intercambio en los últimos años, especialmente en materia de terrorismo y delito organizado, particularmente a partir de los atentados del 11 de septiembre de 2001. También es indicada y condenada por Sepper la circunstancia de establecerse

lazos con organismos de inteligencia de países con gobiernos autoritarios, que obtendrían información bajo tortura, de bajo nivel de confiabilidad.

Frente a ello, la autora citada propuso medidas tales como reafirmar el control sobre los organismos de inteligencia, fortalecer las regulaciones internas sobre tales organismos en relación a la cooperación con sus similares en el mundo, así como los estándares profesionales y éticos vigentes en la materia. También propuso Sepper incrementar la cooperación internacional en materia de inteligencia criminal respecto del delito organizado transnacional e incluso en materia de terrorismo.

Analizando el citado artículo, los autores, compartiendo en general la preocupación de Sepper, expresaron sus dudas en cuanto a la posibilidad de sujetar a un régimen legal estricto la cooperación en materia de inteligencia, ante la característica propia del derecho internacional de carecer de fuerza coercitiva, señalando por otra parte que la autonomía en la toma de decisiones dentro del ámbito de la inteligencia es una característica inherente a dicha actividad, y destacando por otra parte que en la práctica, más que los controles externos ejercidos por órganos legislativos y judiciales, es la *culturización* o transmisión de normas o estándares transmitidos por Estados líderes, lo que produce cumplimiento de las normas internacionales.

Lo que en realidad sobrevuela en el artículo que comentamos -y también en el de Sepper- son las limitaciones que experimenta el control de inteligencia, por las características de la actividad y muy especialmente, por el secreto que protege los tratados y memorandos de entendimiento y sobre todo, la inteligencia obtenida a través de ellos.

A nuestro juicio la carencia de un orden coactivo único en el derecho internacional no es la dificultad fundamental para el control de la cooperación internacional en inteligencia, dado que cada funcionario de inteligencia es responsabilizable conforme a la ley de su propio país, ya sea por actos cometidos en su propio territorio, o en el exterior, en el ejercicio de la función pública<sup>535</sup> – no existiendo, por cierto, inmunidad penal alguna para los funcionarios de inteligencia frente a la ley de su propio país, y ni siquiera respecto de la ley del país del extranjero en que se encuentren, salvo que cuenten con cobertura diplomática, o los acuerdos sobre inmunidad que conciertan algunos países.

## Gestión de Inteligencia en las Américas

En realidad, en materia de cooperación en inteligencia existe para el control una dificultad clásica representada por el secreto, y es que habitualmente, los acuerdos de cooperación en inteligencia, cualquiera sea su jerarquía, formales o informales, incluyen la protección de la inteligencia suministrada por la contraparte, que no puede ser objeto de revelación sin permiso expreso de quien la suministrara. La ruptura de estos acuerdos, además de la responsabilidad ante el país que se entienda perjudicado, tiene como consecuencia el descrédito del país receptor como contraparte en materia de inteligencia.

No podemos sino compartir, en base a la experiencia internacional el escepticismo de Sepper respecto a la eficacia de la transmisión de los estándares y normas de conducta profesionales desde aquellos países líderes a los otros con los cuales interactúan, para lograr la vigencia de los derechos humanos, reconociendo su eficacia en otros aspectos. Suele predominar el interés del país que demanda inteligencia, sin excesiva preocupación respecto de los procedimientos empleados. Los ejemplos citados por Sepper son elocuentes.

Creemos que es posible perfeccionar los controles. Aunque los vigentes en países de alto desarrollo institucional son notablemente superiores a los vigentes en Latinoamérica<sup>536</sup> también tienen limitaciones; muy agudamente, Sepper recuerda que muchos países con controles sofisticados, poseen uno o más organismos de inteligencia con controles mucho menos intensos.<sup>537</sup> Aunque no parece fácil que los tratados sobre cooperación en inteligencia o los memorandos de entendimiento tengan carácter público -como sugiere Sepper- los primeros, que deben ser objeto de ratificación parlamentaria, debieran ser cuidadosamente debatidos en sesiones secretas y los segundos, considerados y examinados por los órganos de control externo e interno de la actividad de inteligencia.

Particularmente el control de la actividad de inteligencia en Latinoamérica requiere drásticas mejoras.<sup>538</sup> También cabe destacar la necesidad, como señala Peter Gill, de que el crecimiento de la cooperación internacional en inteligencia sea acompañado por un crecimiento de la cooperación internacional entre los órganos de control de la actividad.<sup>539</sup>

Uno de los principales problemas antes señalados -la obligación de preservación del secreto de la inteligencia recibida de terceras partes- puede ser en parte encarado favoreciendo la conformación de ámbitos multilaterales



de cooperación en inteligencia, particularmente ámbitos regionales, que incluyan órganos de control multinacional. En materia de cooperación internacional en inteligencia, podemos encontrar un único ejemplo que reúne los caracteres de formal, multinacional, profunda y permanente el de UK/USA – descrito con ejemplar precisión, hace ya tiempo, en el clásico libro *The Ties That Bind*.<sup>540</sup> En el marco de alianzas, pero con menor profundidad, se presentan los casos de la *NATO* y de la Unión Europea, entre otros – sin que la participación en alianzas, frecuentemente, libere a los países miembros de la tentación de producir inteligencia respecto de sus aliados, como lo recuerda Martin S. Alexander.<sup>541</sup>

La cooperación regular en inteligencia, constituye un fenómeno del siglo XX,<sup>542</sup> representando un verdadero *patchwork* de acuerdos multilaterales y bilaterales de todas clases y de todos los grados de intimidad posibles, modulados por los alineamientos políticos de los Estados y sus políticas exteriores.<sup>543</sup> Se está cumpliendo lo afirmado por Gregory F. Treverton, en el sentido de que para la inteligencia estadounidense, “los consumidores se multiplicarían”.<sup>544</sup>

La necesidad de la cooperación en inteligencia deriva de la imposibilidad por parte de un Estado de obtener por sí toda la información necesaria. Por otra parte, al creciente costo de las operaciones de inteligencia se suma la capacidad de algunos organismos de operar con mayor eficacia en ciertas regiones o lugares.<sup>545</sup>

Indudablemente, uno de los factores que influyen en las características que hoy posee la cooperación internacional en inteligencia es la creciente tendencia de empleo de la actividad para auxiliar en la investigación de serios delitos. En América Latina el fenómeno es más intenso aún; organismos de inteligencia con amplias facultades y actividad volcada al interior de sus países. Han dirigido su actividad hacia el delito organizado, disputando terreno con las policías y los organismos de inteligencia criminal.<sup>546</sup>

La actividad de inteligencia de Estado, así como la militar, no son adecuada para investigar delitos. Su personal no conoce las normas procesales para la obtención de pruebas y su incorporación al debido proceso. Sus identidades, fuentes y métodos son secretos; la obvia exigencia de la defensa, e incluso del Ministerio Público y del Juez, por conocer y controlar la forma de obtención de las pruebas, puede representar un serio riesgo para los propios secretos, y

## Gestión de Inteligencia en las Américas

también para los pertenecientes a otros países. Creemos que la actividad de inteligencia no puede sin desnaturalizarse desempeñar un rol policial.

Consideramos por ello que la actividad de inteligencia debe tender a concentrarse en su auténtico rol, que justifica sus ya señaladas características: la protección contra las amenazas para la seguridad del Estado en el interior del país y en el exterior, además de tal protección, la búsqueda de oportunidades para la política exterior del país.

El constante desarrollo de la inteligencia criminal, tanto en el mundo, como en Latinoamérica, así como el idéntico desarrollo de la cooperación subregional, regional e internacional en dicha materia, abre el camino hacia una lucha activa y eficaz y al propio tiempo respetuosa de los derechos humanos, contra el delito organizado e incluso contra el terrorismo, sin negar la subsistencia de un rol para la inteligencia contra este último.

El paulatino establecimiento de ámbitos de cooperación subregional en inteligencia criminal en América Latina<sup>547</sup> marca un camino interesante. También lo ha hecho la Unión Europea en el marco de la cooperación en Justicia y Asuntos del Interior, y especialmente a través de la Constitución de EUROPOL, organismo de inteligencia criminal multinacional de la Unión Europea. EUROPOL constituye un modelo a seguir. Consecuentemente, y como lo señala John Casey, “las estructuras de policiamiento de la Unión Europea son sin lugar a dudas los más fuertes ejemplos de colaboración policial regional”.<sup>548</sup>

La cooperación en inteligencia criminal representa la cooperación entre policías y entre organismos de inteligencia criminal, constituidos fundamentalmente por policías y por analistas sin estado policial. En definitiva, ocurre entre funcionarios conocedores de la legislación penal y procesal penal, así como de la cooperación con los órganos judiciales y con el ministerio público en el proceso penal, con una vigencia mucho más limitada del secreto. El excesivo secretismo existente en el SISP brasileño referido por Priscila Brandão, se debe, en realidad, a la aplicación de una doctrina basada más en conceptos de inteligencia de Estado, que en conceptos propios de la inteligencia criminal.

La construcción de ámbitos institucionalizados subregionales de cooperación en inteligencia criminal concebidos sobre el modelo de EUROPOL, capaces

## Russell G. Swenson y Carolina Sancho Hirane

de encarar eficazmente la diversidad de desafíos y necesidades de cada subregión en Latinoamérica -o bien en *UNASUR* para América del Sur- combinada con un órgano de apoyo hemisférico, podría constituir la base para una lucha eficaz contra el delito organizado transnacional e incluso contra el terrorismo en la región, contribuyendo a superar en ella los riesgos expuestos en el trabajo de Sepper.

**José Manuel Ugarte** es Doctor de la Universidad de Buenos Aires (área Derecho Administrativo), abogado y especialista en Derecho Administrativo y Administración Pública por dicha Universidad, de la que es profesor en grado y postgrado, así como profesor de Derecho Administrativo de la Universidad Católica de Santiago del Estero (DABA), profesor en la Maestría en Derecho Administrativo de la Universidad Abierta Interamericana, y profesor de la Carrera de Especialización en Gestión para la Defensa organizada por la Universidad de Tres de Febrero y la Escuela de Defensa Nacional. Correo: [manuguart@gmail.com](mailto:manuguart@gmail.com).

## Comentarios sobre los Ensayos en la Sección Tres

Thomas C. Bruneau

Cualquiera que sepa algo sobre cómo funcionan realmente las agencias de inteligencia en las nuevas democracias, entenderá que no es fácil tener certeza sobre los temas en detalle a excepción de la naturaleza de sus estructuras formales. También es muy difícil recopilar información confiable. No es sorprendente entonces, que estos tres capítulos se basan en una variedad amplia y distinta de recursos de información incluyendo documentos, libros, artículos, y entrevistas. En vez de ser informes de investigaciones empíricas, estos capítulos buscan expresar en cierto sentido cómo funciona la inteligencia en varios países, con un enfoque particular en Brasil y México. Más específicamente, estos tres capítulos contribuyen a nuestro conocimiento relacionado con el contexto burocrático de estructuras y procedimientos de inteligencia.

El ensayo escrito por Priscila Carlos Brandão demuestra que a pesar de que Brasil ha estado involucrado en un esfuerzo de una década para crear un sistema nuevo de inteligencia, centrado en la Agencia Brasileña de Inteligencia (ABIN), de hecho, todavía hay mucho en el “sistema” que es redundante, superpuesto y opaco. Efectivamente, el sistema de inteligencia de las fuerzas armadas, sobrevive, y todavía tiene un “papel permanente de seguridad interna”, mientras el Servicio de Información Nacional (SIN) -la rama de inteligencia de la dictadura militar que gobernó a Brasil entre 1964 y 1985- fue eliminado a principios de los años 90. Como Brandão señala, es muy importante que en Brasil, la ABIN no tenga la autoridad legal para interceptar llamadas o comunicaciones del internet, sino debe depender de la Policía Federal para estos recursos fundamentales de inteligencia. En mi opinión, esta limitación restringe profundamente la efectividad de la ABIN y puede ser la causa de escándalos interminables, mientras que la agencia intenta compensar esa falta de atribución.

El capítulo escrito por Swenson y Orozco se basa en gran parte en un artículo de Elizabeth Sepper del *Texas International Law Journal* (otoño del 2010) el cual crítica fuertemente el intercambio internacional de inteligencia generalizado y sin control. Los autores así exploran el contexto para el intercambio de inteligencia y se concentran en los fundamentos jurídicos para ciertas actividades de inteligencia. En cuanto a cómo la inteligencia puede

contribuir a la seguridad pública, emplean lecciones principalmente de la experiencia de México. Mirando más específicamente a la Policía Federal Mexicana, demuestran que su competencia y habilidades, en función de los recursos disponibles para ella, varían de estado a estado dentro de ese país, y que las mejoras en inteligencia respecto a la seguridad del ciudadano a nivel local dependerá en encontrar modos éticos para integrar capacidades nacionales y militares de inteligencia junto con la acción preventiva de la policía, tal vez incluso adelante de un marco jurídico nacional por desarrollar.

La contribución de Zúñiga argumenta a favor de la recopilación de inteligencia en el ambiente penal como una actividad legítima, aunque experimental, de mejorar las prácticas de gestión de la recopilación de información del sistema de justicia nacional. Al revisar el marco jurídico para las actividades de inteligencia en distintos países, ella descubre que en Chile, su país de atención, y en la mayoría de los países de la región, la frágil base legal para la recopilación de inteligencia deja mucho espacio institucional libre para la innovación burocrática capaz de promover una expansión razonable de la función de inteligencia.

Lo que sobresalta en estos tres ensayos son varios puntos que nosotros en el Centro para Relaciones Civiles-Militares hemos encontrado que son comunes o típicos en nuestro trabajo en varios gobiernos democráticos recientes. Estos incluyen lo siguiente: Necesitan contar con todos los recursos de información imaginables para comenzar a decir algo sobre la función de inteligencia; existe una ausencia de, o fundamentos jurídicos ambiguos para la función de inteligencia; hay una división confusa de trabajo entre las diferentes agencias de inteligencia, incluyendo las agencias militares y civiles; y además se ve ambigüedad en cuanto a quién hace precisamente qué y a quién se provee el producto final de inteligencia.

Estos estudios también sugieren que un desafío adicional consiste en cómo definir, mucho menos medir, la eficacia de las agencias de inteligencia. Estos son los desafíos que cualquier persona interesada en inteligencia debe tratar, aunque podemos adivinar que nunca puede ser logrado de manera muy satisfactoria.

## Gestión de Inteligencia en las Américas

**Thomas C. Bruneau.** Profesor Distinguido de Asuntos de Seguridad Nacional en la Escuela Naval de Postgrado en Monterrey, California, donde sirve como Administrador del Programa para Latinoamérica y enseña cursos cortos sobre reforma de inteligencia en el Centro de Relaciones Civiles y Militares. Su más reciente libro, coeditado con Florina Cristiana Matei, es *The Routledge Handbook of Civil-Military Relations* (2012). Correo electrónico: tbruneau@nps.edu.



## Os desafios Institucionais no Processo de Integração do Sistema de Inteligência de Segurança Pública Brasileiro

Priscila Carlos Brandão

Neste *paper* temos a oportunidade de analisar o processo de integração do Subsistema de Inteligência de Segurança Pública (SISP) -componente do Sistema Brasileiro de Inteligência (SISBIN)- ao longo da última década. Interessa analisar seu estágio atual, bem como estabelecer propostas que visam aperfeiçoá-lo.

### Legitimidade e eficácia para a inteligência no Brasil

Para haver governabilidade<sup>549</sup> na área de inteligência é necessária uma definição clara de quem a governa, para que, e como se governa. Mas antes de tudo, é preciso fixar de maneira clara o que é inteligência. Ainda que doutrinariamente não exista confusão, na prática, a deficiência da implementação da doutrina na área de segurança pública no país por um lado, e da definição conceitual implícita na doutrina militar por outro, fazem com que a atuação da inteligência se configure como uma zona muito cinzenta no país, marcada por espaços de ambiguidade. Os riscos apresentados pela presença dessa indeterminação são variados, e vão desde a hipertrofia dos poderes, ao sacrifício dos direitos fundamentais, gerando perda de eficácia e eficiência.<sup>550</sup>

Apenas a partir de uma definição amplamente compreendida e legitimada pela sociedade e por aqueles que dela se servem ou a executam, que é possível definir uma direção, um projeto para o setor. O que entra em um segundo ponto de extrema importância sobre o sistema: quem o gerencia, nas perspectivas política e técnica, e quem a executa, no sentido operacional. O gerenciamento do sistema de inteligência, para ser eficiente, depende de fatores externos e internos. Na esfera externa, depende que haja, no âmbito do Poder Executivo, a definição de uma política de inteligência para o país, e de um Plano de inteligência especificamente direcionado para as respectivas áreas. A definição destas políticas e estabelecimento destas metas deve estar afinada com os objetivos de um determinado governo. Ou seja, embora a atividade de inteligência tenha que adquirir uma institucionalidade e legitimidade que a caracterizam como função de Estado, a definição de suas metas estão diretamente relacionadas ao projeto político de um determinado governo.



Depende dos interesses daqueles que são responsáveis pela definição do Plano. A função da atividade é de Estado, mas as definições de prioridades são estabelecidas pelo governante que ocupa o poder em determinado momento. A definição de planos direciona, mas não determina de forma inexorável, as ações a serem desenvolvidas. É preciso haver um determinado grau de flexibilidade, considerando a incerteza do ambiente ao qual nos referimos.

Como argumenta o especialista brasileiro em Estudos Estratégicos, Domício Proença, em recente diálogo com a autora, para governar a inteligência é preciso saber que inteligência é esta, para que serve, para quem, qual o seu custo, quais as salvaguardas lhes são concedidas, quais os limites e controle existentes, e como ela tem sido desempenhada.<sup>551</sup>

Vale esclarecer que estes fatores não podem e nem devem ser resolvidos apenas de forma autônoma, no interior das agências que compõem o sistema, ou pelo próprio sistema, mas deve haver uma adequação entre as políticas definidas no âmbito político, e as metas atribuídas a cada um destes órgãos, considerando sua principal atividade fim.

Por outro lado, dizer que quem governa a inteligência o faz a partir de fora do sistema, não diminui o grau de relevância dos gestores internos, alegadamente, aqueles que têm, ou deveriam ter, além de conhecimentos administrativos, conhecimentos profissionais específicos da atividade, capazes de revelar os recursos e prioridades adequados para seu emprego. O uso dos recursos precisa resultar de uma avaliação conjunta, entre quem governa e quem administra, e deve atender às diversas temporalidades impostas pelas demandas. Nessa avaliação deve ser considerado o que é politicamente satisfatório, com o que é profissionalmente adequado.<sup>552</sup> Emerge destas considerações, o conceito de eficiência na gestão da função de inteligência.

### Inteligência na área de segurança pública

O debate na Ciência Política sobre as funções da atividade de inteligência, sobretudo da inteligência criminal em contextos democráticos, tem sido marcante na América Latina, a exemplo da discussão apresentada pelo cientista político argentino, no início do milênio:

Colocando como centro el afianzamiento de la gobernabilidad, la formulación e implementación de políticas destinadas

## Gestão de Inteligência em las Américas

a atender los problemas vinculados a la seguridad pública debe superar la visión unívoca y reduccionista de seguridad = policía, o seguridad = represión, para integrarse en un esfuerzo común en donde las políticas de seguridad y la política criminal, se conjugan en el marco de la dimensión social.<sup>533</sup>

No setor de Segurança Pública no Brasil, a complexidade de áreas abrangidas pela atividade de inteligência interna dentro do contexto da Segurança Institucional demanda alguns esclarecimentos. De acordo com relevante parte da literatura internacional, a inteligência interna subdivide-se em duas áreas. Primeiro, a inteligência de segurança (*security intelligence*), ou inteligência doméstica (*domestic intelligence*), como conhecida no caso dos Estados Unidos, relacionada à identificação de ameaças potenciais à segurança do Estado. A segunda é a área de inteligência criminal (*criminal intelligence*), conhecida nos Estados Unidos como Inteligência para a Imposição da Lei (*Law Enforcement Intelligence/LEI*), e está relacionada ao apoio às funções investigativas policiais e ao provimento da ordem pública e justiça criminal. Entretanto, no Brasil, as funções compreendidas na esfera da segurança interna (inteligência de segurança doméstica e inteligência criminal), encontram-se imiscuídas na definição de Inteligência de Segurança Pública. O problema desta mescla não é relativo a uma necessidade de pura reprodução taxonômica, e sim, ao desafio que acarreta para o desempenho eficiente da atividade, e à capacidade de gestão dos sistemas de inteligência.

Em seu trabalho *Segurança tem saída* (2006), Luiz Eduardo Soares estabeleceu um diagnóstico sobre a segurança pública no país e destacou dois grandes problemas: a péssima qualidade da gestão no setor, e a obsolência das estruturas corporativas.<sup>554</sup> Para o autor, um modelo de gestão empresarial seria uma condição necessária, ainda que não suficiente, para se pensar em realizar uma condução *eficiente* da política de segurança pública no Brasil: “conhecendo o problema para o qual tem que oferecer resposta; planejando o que vai ser feito; avaliando o que foi feito; identificando erros e acertos, e monitorando todo o circuito”.<sup>555</sup>

Vários fatores são ponderados por Soares. O fato de os gestores das organizações não terem formação e nem conhecimento na área administrativa; de os cargos administrativos não terem como base competência e confiança; de as nossas instituições de segurança pública serem refratárias a alterações;

bem como o fato de serem corporativistas, a relação entre as corporações, que deveriam agir em cooperação, são marcadas por rivalidade e disputas mesquinhas.<sup>556</sup>

Ao analisar este apego conservador ao corporativismo, Soares clama pela necessidade de se compreender quais reformas são necessárias para a construção de um sistema de segurança pública eficiente. Segundo o balanço do autor:

Nossas polícias são máquinas pesadas e lentas, nada inteligentes e criativas, que não valorizam seus policiais e nem preparam adequadamente, não planejam nem avaliam o que fazem, não aprendem com os erros porque não os identificam, não conhecem os problemas sobre os quais atuam (os policiais, individualmente, sabem muito, a polícia, como instituição, nada sabe); não cultivam o respeito e a confiança da população (...); cometem um número imenso de crimes, quando sua tarefa é evitá-los ou conduzir à Justiça os perpetradores.<sup>557</sup>

Para além de toda a rivalidade, ainda destaca problemas estruturais que dificultam a cooperação. O primeiro seria a falta de padronização de um sistema de comunicação profissional, que permitisse um adequado compartilhamento de dados, sempre úteis para a produção de inteligência na área de segurança pública. Cada polícia tem seu modo próprio de formar seus quadros, com cursos realizados em prazos e formatos distintos, não há nem mesmo um ciclo básico comum. Cada uma das polícias tem modo próprio de classificação de informações, dificultando o processo de interação. Não há um sistema nacional efetivo que organize estas instituições, as quais comportam-se como unidades isoladas que se rivalizam e raramente cooperam entre si. Até mesmo no âmbito das polícias abrigadas no Ministério da Justiça, -Polícia Federal e Polícia Rodoviária Federal- pouco diálogo existe. Diante deste cenário ineficaz, Soares questiona: como seria possível criar uma cultura profissional, um sistema *eficiente*, amparado em uma linguagem técnica capaz de ser compartilhada?<sup>558</sup>

Considerando as premissas estabelecidas pelo autor em 2006 e válidas para 2012, de que para o começo de um processo de mudança salutar para o sistema de segurança pública do país é necessário desenvolver um planejamento efetivo, capacitação, avaliação sistemática, valorização dos profissionais,

## Gestão de Inteligência em las Américas

avaliação dos procedimentos e controle, quais propostas práticas, no campo de inteligência, poderiam ser pensadas para reforçar a reforma e integração dos órgãos responsáveis pela atividade no setor de segurança pública, cujos problemas são apenas reflexos deste caos anteriormente narrado? Antes de seguirmos às propostas propriamente ditas, passemos a uma revisão crítica do cenário institucional atual, o qual ainda não desenvolveu uma reforma consistente para a produção de um sistema menos corporativista. O que não implica que esta reforma não seja possível e não esteja, ainda que a passos lentos, em andamento.

### A institucionalização do Subsistema de Inteligência da Segurança Pública

Em 20 de junho de 2000, durante a gestão do Presidente Fernando Henrique Cardoso, foi divulgado o *Plano Nacional de Segurança Pública/PNSP*, que em seu Compromisso No 4 previa a implementação do Subsistema de Inteligência de Segurança Pública/SISP, no âmbito do Sistema Brasileiro de Inteligência, a ser integrado por órgãos das esferas “federal, estadual e municipal, tendo por objetivo identificar ameaças à segurança pública, subsidiar, (...) com conhecimentos necessários, a adoção de providências para a manutenção da segurança pública.”<sup>559</sup>

Inicialmente, o SISP foi regulamentado por meio do Decreto 3.448, de 05 de maio de 2000, tendo a ABIN [Agência Brasileira de Inteligência (no país, a agência possui responsabilidades tanto em relação à área externa, quanto interna, com amplo predomínio da última)] como órgão central, e seu diretor-geral como presidente. Não obstante, em meio a uma disputa de poderes envolvendo o Ministério da Justiça/MJ e o Gabinete de Segurança Institucional/GSI, viabilizada pela generalidade com que os conceitos de inteligência e de sistema foram tratados na lei que regulamentou o SISBIN,<sup>560</sup> um novo decreto foi elaborado, retirando da ABIN o posto de órgão central do SISP, atribuindo-lhe à Secretaria Nacional de Segurança Pública/SENASP-MJ.<sup>561</sup> Caberia ao SISP “coordenar e integrar as atividades de ISP em todo o país, bem como suprir os governos federal e estaduais de informações que subsidiem a tomada de decisões neste campo.” (Art 1o).

Além da SENASP, como seu órgão central, o SISP, possui como componentes operacionais os Departamentos de Polícia Federal/DPF e a Polícia Rodoviária

Federal/DPRE, no âmbito do MJ; além de alguns órgãos do Ministério da Fazenda; do Ministério da Integração Regional; do Ministério da Defesa; do GSI (ABIN e Secretaria Nacional Antidrogas/SENAD), além das polícias civis e militares<sup>562</sup> dos 26 Estados e do Distrito Federal, esses últimos, integrados mediante convênios.

Caberia aos representantes do SISP “identificar, acompanhar e avaliar ameaças reais ou potenciais de segurança pública e produzir conhecimentos e informações que subsidiem ações para neutralizar, coibir e reprimir atos criminosos de qualquer natureza.” (Arto 2, §3). Ainda que se tratasse de um conceito vago, tornou-se o único conceito disponível para orientar os debates em torno dos marcos doutrinários e regulatórios a partir de então produzidos.

O decreto também determinou a criação do Conselho Especial do Subsistema de Inteligência de Segurança Pública (CE/SISP), órgão de deliberação coletiva, com a finalidade de estabelecer normas para as atividades de inteligência de segurança pública/ISP (Art 3o). Como membros permanentes estavam o Secretário Nacional de Segurança Pública (responsável por presidi-lo) e os representantes dos órgãos acima mencionados, à exceção dos estados, que participariam apenas como membros eventuais, sem direito a voto.

Em dezembro de 2001 a Secretaria Nacional de Segurança Pública promoveu o *I Seminário Nacional sobre a atividade de Inteligência de Segurança Pública*.<sup>563</sup> Entre as posições consensuadas, a ISP foi apresentada como uma ferramenta de *análise* de fenômenos relacionados à segurança pública, entre os quais se destacam a identificação da forma e atuação de organizações criminosas e das novas modalidades de crimes, a elaboração do perfil das pessoas envolvidas, sejam autores ou vítimas, para *auxiliar* na solução de procedimentos investigatórios policiais, além de *subsidiar* o planejamento da gestão de segurança pública, através do fornecimento de dados, informações e conhecimentos.<sup>564</sup> Em relação ao “estado da arte” dos órgãos de inteligência estaduais, foi constatado que não se tratava de sistema formalizado na maioria dos Estados, reforçando a necessidade de viabilizar o ajuste das estruturas existentes e o desenvolvimento de determinado grau de padronização. Também foi constatada a deficiência da qualificação profissional na área, a carência de equipamentos específicos para o desempenho da atividade, a necessidade do desenvolvimento de uma mentalidade de inteligência compatível com os objetivos do Plano Nacional de Segurança Pública e com os preceitos legais

## Gestão de Inteligência em las Américas

vigentes, a ausência de doutrina específica para a ISP, e por fim, a ineficiência das medidas de contra-inteligência.

Entre os principais desafios do funcionamento dos sistemas estaduais de ISP, destacou-se a necessidade de estabelecimento de uma “mão-dupla” no fluxo informacional entre os órgãos estaduais e federais componentes do SISP, a instituição de mecanismos que possibilitassem a ligação técnica entre os órgãos de inteligência vinculados hierarquicamente a secretarias distintas, e a manutenção de um sistema voltado única e exclusivamente para a área de segurança pública. Em termos de capacitação foi constatada a necessidade de formar profissionais e aperfeiçoar os policiais para a área de ISP. Sobre os procedimentos relacionados à interceptação telefônica foi relatada uma série de dificuldades encontradas pelos operadores, bem como fornecidos subsídios para a reelaboração de um novo marco regulatório. Por fim, em relação à discussão sobre projetos estaduais da área de ISP, foi sugerido que se realizasse treinamento dos recursos humanos, observando-se o perfil do futuro profissional da área de ISP, buscando-se aperfeiçoar os profissionais de ISP dos órgãos existentes, e proporcionar seus devidos aparelhamento/reaparelhamentos.<sup>565</sup>

O Grupo de Trabalho responsável pela elaboração da doutrina finalizou seu trabalho em 2001, cujo desenho, de acordo com as conversações estabelecidas entre autora com alguns participantes, refletia as Orientações Doutrinárias do SISBIN, utilizada pela ABIN (que tampouco possuía uma “Doutrina” regulamentada).

Em um segundo seminário sobre ISP promovido em 2002, a SENASP divulgou a criação, bem como procurou fomentar sua utilização sistemática, da Rede Nacional de Informações de Segurança Pública (RENISP).<sup>566</sup> A RENISP foi a solução tecnológica criada para a transmissão de dados, na modalidade criptografada, instalada em todos os órgãos que compunham o SISP. Foi paulatinamente implementada, face à dependência da adesão dos estados.

A partir de 2003, com a entrada do sociólogo Dr. Luis Eduardo Soares na condução da Secretaria Nacional de Segurança Pública, vários esforços foram empreendidos, no sentido de promover interação/integração, a exemplo da criação da Coordenadoria Geral de Inteligência,<sup>567</sup> e capacitação

dos profissionais da área. Para tanto, foi elaborado o primeiro Curso de Aperfeiçoamento de Inteligência de Segurança Pública/CAISP, projetado pelo estado em parceria com especialistas do país na área, cujo processo de criação e implementação foi muito rico, dada a natureza das ferramentas oferecidas.<sup>568</sup>

Elogiado por uns, criticado por seus “academicismos” por outros, o primeiro curso de impacto promovido pela Secretaria Nacional de Segurança Pública foi capaz de fincar raízes e iniciar um processo de interação, ainda que informal, entre componentes dos vários órgãos do sistema, ensejando, posteriormente, a criação do Instituto de Inteligência Criminal (INTECRIM) e do atual Capítulo Brasil do *International Association of Law Enforcement Intelligence Analysts (IALEIA)*. Entretanto, a dramática saída do secretário nacional Luis Eduardo Soares ainda em 2003, somado ao descaso com que o encerramento do curso foi tratado pelo novo secretário,<sup>569</sup> relegaram o curso ao quase esquecimento.

Posteriormente, a sobreposição de funções que ocorreu na Coordenadoria Geral de Inteligência (CGI) no período da organização dos Jogos Pan-Americanos de 2007, o reduzido tamanho da equipe, a falta de prioridade com que o tema inteligência foi e ainda é tratado nas esferas políticas (não obstante seja sempre apresentado como a solução de todos os problemas para a segurança pública), emperrou o processo de encerramento da doutrina, que havia sido vencido em sua etapa mais difícil, a que dependia da interlocução dos operadores do sistema. E foi neste momento que a gestão da CGI, diante da necessidade de apresentar os retornos em termos de investimentos financeiros e políticos produzidos ao longo dos dois períodos de debate, encerrou esta segunda fase, aprovando a Doutrina Nacional de Inteligência de Segurança Pública/DNISP, junto a uma minoria dos membros que a debateram, suprimindo-lhe vários itens, e divulgando-a, ostensivamente, sem que um acordo para tanto, tivesse sido realizado. A terceira fase tem seu capítulo final com a aprovação da DNISP junto ao Conselho Especial/CE em 22 de julho de 2009,<sup>570</sup> na gestão do secretário Ricardo Balestreri.

A aprovação da DNISP junto ao Conselho Especial durante a gestão do delegado Luiz Fernando Corrêa (2003/2007) como Secretário Nacional de Segurança Pública, havia sido indefinidamente postergada, considerando-se o envolvimento da CGI com a segurança dos Jogos Pan-Americanos, e a expectativa que foi criada por esta gestão, junto aos representantes estaduais,

## Gestão de Inteligência em las Américas

de levar ao CE uma proposta de reformulação da legislação para a área de inteligência de segurança pública, que incluísse a participação plena dos representantes estaduais junto ao Conselho. Esta iniciativa foi realmente executada, a proposta foi levada ao CE e aprovada em reunião realizada aos 5 de abril de 2005.<sup>571</sup> No entanto, não chegou a ser politicamente implementada, uma vez que dependia da apresentação de um Projeto-Lei junto ao Congresso Nacional, de iniciativa do Poder Executivo, que alterasse a Lei 3695, o que nunca foi realizado. Tal inércia na condução da proposta de alteração nos deixa em dúvida se a apresentação da proposta junto ao CE teria sido apenas uma manobra para acalmar os ânimos dos representantes estaduais, ou se havia, de fato, interesse na alteração. No que tange a este debate, a segunda gestão mais duradoura da CGI (órgão da Secretaria Nacional de Segurança Pública responsável pela integração dos operadores de inteligência) no governo Lula, conduzida pelo então secretário Ricardo Balestreri, foi marcada por uma postura política explicitamente mais “precavida” do que a anterior, no sentido de evitar se tornar refém de qualquer pacto político que pudesse ocorrer entre os estados na área de ISP, e postulou um papel mais efetivo de representante dos interesses estaduais, ao criar o Conselho Nacional de Chefes de Organismos de Inteligência (CNCOI).<sup>572</sup>

Outro processo “deixado pelo caminho” pela gestão de Luiz Fernando Corrêa foi a institucionalização dos Cursos de Especialização de Inteligência de Segurança Pública. Em 2006, por iniciativa dos gestores do setor de inteligência de segurança pública do estado do Mato Grosso, foi realizado o primeiro curso de especialização em Inteligência de Segurança Pública do país. Tratou-se de um projeto piloto, previsto para ser reproduzido em outros estados, cujo retorno imediato em termo de investimentos foi a promoção de uma efetiva interlocução dentro do subsistema de inteligência estadual, realizado a partir da interação entre seus componentes/alunos.<sup>573</sup> Não obstante, assim que iniciaram as tratativas para a segurança dos Jogos Pan-Americanos, a prioridade relativa ao profissionalismo e a integração do SISP foi abandonada.

A gestão da CGI (Coordenadoria Geral de Inteligência) no período do Secretário Balestreri apresentou maior interesse (modo geral, a equipe como um todo), em imprimir um processo menos reativo e menos pautado por uma política de barganhas. Entre 2008 e 2009, sobretudo, promoveu uma nova formatação para o banco de dados sobre informações criminais, o Sistema



Nacional de Informações de Justiça e de Segurança Pública (INFOSEG), que foi transformado em uma rede, a Rede de Integração Nacional de Informações de Segurança Pública; alterou o modo de acesso à RENISP, que passou a ocorrer por meio de um modelo pendrive criptografado, promovendo mais flexibilidade; criou o Conselho Nacional de Chefes de Organismos de Inteligência, (um conselho representativo dos estados junto ao Conselho Especial do Secretária de Inteligência de Segurança Pública); e promoveu uma regulamentação *efetiva* da doutrina.

A exemplo do que ocorreu anteriormente, a CGI também teve seu processo de implementação de políticas de capacitação e integração do sistema preterido em função de sua atuação na articulação do sistema de segurança da agenda esportiva do país, as novas preocupações ocorreriam em torno dos Jogos Olímpicos (2016) e da Copa do Mundo de futebol (2014). Mas sem dúvida, a atuação desta gestão implementou passos importantíssimos para o processo de institucionalização da Secretaria de Inteligência de Segurança Pública, apesar de aquém das promessas de integração e capacitação esperadas.

### Atividade de inteligência de segurança pública: doutrina e conceito

Explicitarei com riqueza de detalhes as negociações, demandas e sugestões elaboradas pelos gestores em torno do tema Inteligência de Segurança Pública. Entre os debates estabelecidos, um tema que alcançou consenso em meio a uma discussão conflitiva e desgastante, diz respeito ao entendimento sobre a função da atividade no país. Ficou claro nos debates, que a atividade possui função *subsidiária*, produz conhecimento para *auxiliar* o tomador de decisão ou para *subsidiar* policiais responsáveis por produzir a prova. São finalidades da inteligência de segurança pública, entre outras, apoiar diretamente, com *informações relevantes*, as operações policiais de prevenção, patrulhamento ostensivo e investigação criminal e *auxiliar na investigação* de delitos.<sup>574</sup>

Entretanto, entender que a inteligência policial não tem como atividade fim a produção de provas, e sim, de conhecimentos, tem sido um dos maiores desafios empíricos do sistema. Os documentos produzidos na área de inteligência normalmente são classificados ou restritos, bem como seus operadores estão sujeitos a sigilos funcionais, e para que se tornem prova é preciso desclassificá-los, expor os métodos, técnicas e agentes da área, acarretando um custo altíssimo

## Gestão de Inteligência em las Américas

para a produção desta prova. Compreender os limites entre inteligência em sua fase pré-delitual e pós-delitual tem sido um dos grandes dilemas no país, principalmente porque, uma vez explicitados, são delimitados os responsáveis e os meios disponíveis para sua produção.

Por mais paradoxal que pareça, apesar da existência da Lei 9296, de 24 de julho de 1996, que regula a possibilidade de realização da interceptação telefônica no país, foi apenas a partir da aprovação da Doutrina Nacional de Inteligência de Segurança Pública em 2009, que ficou explícito que é vedado aos responsáveis pela atividade de inteligência a realização de interceptações que não ocorram no âmbito de uma investigação. As *Ações de Inteligência Policial (judiciária)* definidas na doutrina são aquelas que envolvem o emprego de técnicas especiais que visam a obtenção de dados negados e dependem de autorização judicial (constituem-se de indícios, evidências ou provas de autoria ou materialidade de um crime), a qual é concedida apenas no decorrer de uma investigação. O resto do sistema que desenvolve a atividade de inteligência de segurança pública no país, o que inclui segurança interna, não possui os mandatos necessários para o cumprimento de suas funções, evidenciando a fragilidade de nossa legislação. Diferentemente do *Federal Bureau of Investigation* dos Estados Unidos, que após os atentados de 11 de setembro de 2001 passou a acumular novas e grandes capacidades de inteligência doméstica e inteligência criminal,<sup>575</sup> a Polícia Federal, para desencadear o processamento de informações e produção de análises relativas à penetração de supostos membros de uma rede terrorista no país, não possui os mandatos relativos à coleta intrusiva, a não ser que já tenha sido identificado um crime precedente, como por exemplo, tráfico de armas, lavagem de dinheiro etc. Assim como a ABIN também não. A falta de mandados, considerando todos os princípios que devem regê-los (legitimidade, proporcionalidade etc.) esvazia o potencial destas funções na esfera da pró-atividade e da contra-inteligência no país. Daí a resistência inicial dos militares e da ABIN à criação de uma doutrina especificamente voltada para a área de segurança pública.

Por outro lado, a Constituição do país permite aos militares, como missão secundária das Forças Armadas, atuarem em defesa da lei e da ordem. Neste sentido, ainda que atualmente o conceito de “inimigo interno”, característico da Guerra Fria, não conste na atual Política de Defesa Nacional, sua permanência durante várias décadas como principal pilar das políticas militares, com destaque para o período da ditadura, faz com que ainda exerça

grande influência na definição das ações do setor de inteligência militar. No país é muito significativo o fato de que pouquíssimo esforço foi realizado pelos governos civis após a transição, no sentido de produzir um conceito que esclarecesse quais situações ou atores poderiam ser definidos como ameaça, e estabelecesse a diferença entre defesa interna, segurança, e defesa do Estado de Direito.

O Capítulo XVI do Decreto 7364/10, que regulamenta a estrutura do Ministério da Defesa, reconhece que é competência das Forças Armadas, “quando couber”, a “garantia da lei e da ordem, visando a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, na garantia da votação e da apuração eleitoral, bem como sua cooperação com o desenvolvimento nacional e a defesa civil e no combate a delitos transfronteiriços e ambientais”.<sup>576</sup> Esta disposição infra constitucional é delimitada em sua maior parte pelos próprios militares que a interpretam, basicamente ignorando o “quando couber” ou “a iniciativa de qualquer um destes”, e o traduzem em capacidades permanentes das Forças Armadas.

A definição de área de competência do Ministério da Defesa/MD, que vai desde a função de polícia nas fronteiras, garantia da ordem, defesa das pessoas e do patrimônio, à garantia da apuração eleitoral e da defesa civil, se bem que minimiza-se a capacidade da inteligência militar no que diz respeito à sua atividade fim, visto que seus recursos humanos, tecnológicos e orçamentários são restritos,<sup>577</sup> transforma o MD em um dos elementos mais maleáveis da estrutura administrativa, utilizável em todos os momentos em que o Estado é incompetente, a partir dos órgãos apropriados, de cumprir sua função.

Vale ressaltar que nos últimos anos, a Doutrina de Segurança Nacional passou por diversas adaptações no Brasil. Contudo, conforme é possível perceber no discurso militar ainda presente, sua característica fundamental é o conflito permanente, e é esse quadro de conflito que subordinava e ainda subordina as demais atividades, à lógica de segurança do Estado, em detrimento da segurança individual.

Recentemente a Revista *Carta Capital* (19/10/2011), de grande circulação e prestígio no país, divulgou trechos de um documento intitulado “Manual de Campanha – Contra-Inteligência”, que nos fornece indícios inequívocos sobre a permanência deste tipo de mentalidade, e de como as expressões são manipuladas, de forma a legitimar e justificar a atuação dos militares, junto

## Gestión de Inteligencia en las Américas

às esferas internas. Não negamos de maneira alguma a necessidade de um Manual de Contra-Inteligência, como também não negamos a presença de pseudo-ONGs no país, a existência de biopirataria etc. No entanto, temos que atribuir a César, o que é de César. Em trecho que define quais atores devem ser considerados “Elementos Adversos”, esclarece o Manual:

Grupos, movimentos sociais, entidades e organizações não governamentais e mesmo órgãos governamentais, de cunho ideológico ou não – atuando no país e no exterior – ou por segmentos autônomos, elementos radicais ou a eles vinculados, que defendem mudanças radicais e revolucionárias, ultrapassando, em seus programas e bases doutrinárias de caráter político-ideológicas, religiosas e étnicas, *os limites da legalidade institucional* do Estado democrático de direito, e *cujos procedimentos ilegais possam vir a comprometer a ordem pública e até mesmo a ordem interna do país*.<sup>578</sup>

Ao mesmo tempo em que procura legitimar a atuação das forças armadas no campo interno, a partir do momento em que estas forças adversas *ultrapassem* os limites da legalidade institucional e cuja ação possa vir a comprometer a ordem pública ou a ordem interna do país, nitidamente ignora o princípio da proporcionalidade, ao colocá-los como elementos continuamente passíveis de acompanhamento, a não ser que consideremos a ação do Movimento dos Sem Terra (MST) ou a Greve dos Correios, por exemplo, uma ameaça tão grave à institucionalidade do país, que não possa ser acompanhada pelos órgãos de inteligência do setor de segurança pública. Aliás, mesmo no que tange ao acompanhamento destes movimentos por parte dos órgãos civis de inteligência, ainda é possível questionar algumas de suas validades, em um Estado democrático de direito. Algo está errado ao se naturalizar estes componentes, marcadamente característicos de um Estado autoritário, o qual não suporta a adversidade de opiniões. Assumir a necessidade da atuação das Forças Armadas nesta esfera de atuação seria como assumir que somos um Estado incapaz de lidar com a própria dinâmica de governabilidade de um país democrático.

Segundo Domício Proença Júnior e Eugênio Diniz, a Doutrina de Segurança Nacional (DSN) ainda deslegitima a divergência de opiniões e demoniza o conflito, impossibilitando o debate democrático. Suprime, de forma simplória, a complexidade do processo decisório das sociedades modernas, seja

numa ditadura, seja numa democracia.<sup>579</sup> É crucial esclarecer que a crítica aos entendimentos nascidos da DSN não se encerra em condições principais, em sua inadequação à democracia, ou seu apego a considerações pseudo-científicas, cabalmente desmentidas pela história. De acordo com os autores, a crítica à DSN é imprescindível em função do risco real que sua aplicação pode trazer à busca de metas políticas – para a gestão concreta dos assuntos de segurança e defesa.<sup>580</sup>

Priorizar o campo interno significa orientar o potencial das forças armadas para uma missão que lhe é secundária. E considerando o protagonismo que o país vem assumindo paulatinamente no cenário internacional, isto é inadmissível. Não há dúvidas de que urge um processo de transformação e modernização do nosso modelo de inteligência e sua adequação aos temas tais como terrorismo (muito diferente do termo subversão, do qual os militares tem um grande apreço), e espionagem estrangeira.<sup>581</sup>

### Inteligência de segurança pública, inteligência policial e investigação policial

Critério unificador entre investigação policial e análise investigativa de inteligência, é que ambas estão condicionadas pelas regras jurídicas que balizam a admissibilidade das provas. Aspecto diferenciador, é que a inteligência policial produz conhecimento que confirma evidências, indícios ou provas que possibilitem identificar a autoria e materialidade do crime, e que seu trabalho não se encerra com a investigação. Na inteligência policial, existe um sistema de retroalimentação de informação, que desencadeia um processo cíclico de produção de conhecimento de inteligência. A partir do momento que são coletadas novas informações e novas análises são produzidas, aumenta-se a possibilidade de se desencadear novas investigações e aí sucessivamente, transformando a análise investigativa em análise estratégica. Segundo Mônica Lacerda, “o produto do seu processo analítico integra-se a um banco de dados e é utilizado para a previsão e prevenção de eventos indesejáveis, neste sentido, não atuando mais como inteligência policial investigativa, mas preventiva”.<sup>582</sup>

No caso das operações de inteligência de segurança pública voltadas para a prevenção de delitos, crimes e graves perturbações da ordem pública (análise estratégica), operações muitas vezes levadas a cabo pela polícia ostensiva no

## Gestão de Inteligência em las Américas

Brasil, e não pela polícia investigativa, os parâmetros para a admissibilidade da utilização de meios intrusivos de busca de dados negados são muito menos claros. A atividade se manifesta no âmbito extra penal, no qual as regras ainda são difusas e imprecisas e, por conseguinte, prevalece um leque de opções e decisões mais discricionário para o gestor público.

As possibilidades de minimizar as ameaças implícitas no desenvolvimento da atividade de inteligência de segurança pública em sua função estratégica estão diretamente relacionadas à capacidade da autoridade administrativa competente, baseada em parâmetros normativos específicos, de direcionar a atividade de inteligência. A gestão eficaz da função depende de coibir o uso de métodos intrusivos e fomentar a capacitação dos analistas, de modo a maximizar o processo de produção de inteligência baseado em fontes ostensivas e bancos de dados organizados de forma inteligente e compreensível.

### Propostas práticas no campo de inteligência para reforçar a reforma do setor de segurança pública

Fórmula indiscutível para potencializar a capacidade de inteligência de segurança pública no país está relacionada ao processo de institucionalização da prática de intercâmbio informal de dados, realizada entre os vários seguimentos vinculados à área, independentemente do tipo de instituição e da prática de policiamento, se ostensivo ou preventivo.

Em seu recente trabalho, *The Blue Planet*, Michael Bayer (2010) buscou comprovar como a não absorção das capacidades produzidas por meio da troca informal de dados, realizadas entre agências policiais de todo o mundo, tem sido um dos maiores equívocos da campanha de combate ao terrorismo promovido pelos estadunidenses: “*formal relationships are helpful, informal relationships are powerful*”.<sup>583</sup> Segundo o autor, algumas características inerentes dos órgãos policiais as transformam no mais potente instrumento de combate à criminalidade complexa e, por extensão, ao terrorismo. Sob esta lógica, para que as ações terroristas sejam desencadeadas, várias ações criminosas são anteriormente realizadas, de forma a viabilizar sua consecução material: tráfico de drogas, de pessoas, extorsão, lavagem de dinheiro, comércio ilegal de armas e outras. Estas ações constituem o foco de ação das agências policiais.

Ainda que as premissas apresentadas pelo autor sejam válidas, sobretudo para a interação entre agências de países distintos (ou seja, que não disputam entre si poder, orçamento e capacidade de influência), podem ser estabelecidas como metas de comportamento para as agências policiais brasileiras, vistas como um referencial para o estabelecimento de uma grande rede, capaz de viabilizar um tipo de coleta que o autor qualifica como “um arrastão” de dados de vários tipos.

Entre as principais premissas colocadas pelo autor destacamos: 1) a capacidade que a polícia tem de se adaptar, ajustar e agir rapidamente, no sentido de alcançar respostas que demandam ação imediata;<sup>584</sup> 2) o fato de que existe um sentimento de pertencimento entre as várias corporações policiais, considerando que têm missões em comum – manutenção da segurança e da ordem –, e inimigos comuns – os criminosos, que os estimula a cooperar entre si (neste sentido, o autor interpreta o corporativismo policial a partir de seu lado positivo, a “*Culture of the badge*” exprimiria uma tendência à cooperação entre órgãos similares);<sup>585</sup> 3) a capilaridade destas agências é outro fator positivo, pois permite aos policiais atuarem nos mais variados níveis (estadual, federal, local), nos mais distintos lugares (metrópoles, vilas, bairros, guetos), sendo que esta cooperação transcende religiões, etnias, preferências políticas, e outras fronteiras que poderiam inviabilizar a cooperação. Daí a atuação em todo *The Blue Planet!* É justamente em função desta capilaridade, acrescidos do *know how* em investigações, que as agências policiais, por meio de seus contatos informais, têm uma capacidade única de “ligar os pontos”;<sup>586</sup> 4) a independência que possuem em relação aos centros de poder – principalmente se comparados aos serviços de inteligência, eles mesmos órgãos de poder de um determinado governo –, o que permite uma autonomia mínima, necessária para o desenvolvimento das missões destas agências.<sup>587</sup>

Em resumo, o sentimento de pertencimento, a independência em relação aos centros de poder, e a capilaridade devem ser observados enquanto instrumentos de extrema importância para o combate à criminalidade do país. Tais premissas representariam um conjunto de condições necessárias para a troca de informações, ainda que não suficientes. A promoção de um intercâmbio fluente de informações entre policiais também demanda confiança, a base de todo o processo de circulação da informação. Segundo Bayer, dois fatores são fundamentais para imprimir confiança: o sentimento de pertencimento (presumido) e a reciprocidade.<sup>588</sup> Para que dados circulem de maneira

## Gestão de Inteligência em las Américas

informal é preciso, ou que já tenha havido contato entre agentes, ou que, amparado na expectativa de que quando necessário será possível contar com a ajuda daquele que pede auxílio, um agente sempre ajudará seu colega.

Interessante destacar que no país tanto os policiais quanto outros agentes da área de inteligência de segurança pública sabem o valor e a importância de se compilar e acessar determinados bancos de dados, da necessidade de um fluxo informacional multidirecional, e no entanto, fatores variados ainda fazem com que as agências policiais não cooperem entre si, privilegiando o lado negativo do corporativismo, ou seja, a disputa de território, em detrimento do cumprimento de sua missão primária: a segurança dos cidadãos.

Mas porque privilegiar a troca informal de dados? Em primeiro lugar, as informações divulgadas por meios informais (baseadas na confiança ou no voto de confiança), muitas vezes enriquecem os dados já disponibilizados por canais burocráticos. Em segundo lugar, o ritmo da troca burocrática de informações não atende a necessidade de agilidade dos órgãos policiais. Requerimentos realizados por meios formais demandam muito tempo para ser atendidos, necessitam ser escritos, transmitidos, registrados, analisados, debatidos, considerados, aprovados ou desaprovados, para daí serem ou não respondidos. Isto pode levar dias, semanas, meses. A troca de informações entre policiais, feita “*cop to cop*”, pode levar minutos, o tempo de um telefonema, uma troca de fax, de um e-mail etc. E em uma dinâmica que depende de informações disponíveis, para que um caso “não esfrie” ou que alguém mais seja prejudicado, o fator tempo é crucial.

Bayer procura demonstrar em seu livro como, ao transferir a lógica de funcionamento das *ummahs* para o mundo globalizado, instituições como a Al-Qaida tiraram muito mais proveito da tecnologia de comunicações, do que os próprios estadunidenses.<sup>589</sup> As unidades sociais islâmicas, denominadas *ummahs*, guardam relação com a ideia árabe de *asabiyah*, que se refere a um tipo de solidariedade social, à consciência de grupo, a uma coesão, no sentido de pertencimento, identidade. E foi justamente por meio desta lógica, que estabeleceram uma fantástica rede, de transmissão segura de comunicações, ainda que informal.

Mas também não bastam apenas a noção de pertencimento e a confiança, há no país outra lógica que precisa ser invertida: a de compartimentação, para



a de interação. É preciso promover o compartilhamento, e neste sentido, as agências policiais têm mais uma vantagem sobre os órgãos de inteligência: os órgãos policiais, diferente das esferas de inteligência, produzem informações que são, obrigatoriamente, produzidas em obediência às regras do direito penal. Os parâmetros para a admissibilidade da utilização de meios intrusivos de busca de dados negados são muito claros, o que gera informações muito mais confiáveis. E se a informação dos colegas, ainda que à distância pode ser confiável, então é factível a reciprocidade entre agentes de um mesmo país, a troca em tese é mais atrativa, pois o interesse é comum.

Esta inversão da cultura de compartimentação necessita ser realizada tanto extra, quanto intra-muros. Dentro de uma mesma instituição, a informação muitas vezes não circula, é privatizada enquanto instrumento de poder de determinadas autoridades. Não obstante, fato consumado é que a globalização e a expansão tecnológica promoveram maior autonomia para as esferas intermediárias no que diz respeito ao acesso à informação, e neste sentido, houve um determinado deslocamento do poder. Isto não implica desordem e desobediência hierárquica, pelo contrário, apenas reforça o papel das chefias no desenho e estímulo à criação de sistemas de troca de informação. Informação retida desnecessariamente não deve ser entendida como aumento de poder pessoal, e sim, como perda de possibilidade de atuação eficaz e eficiente.

Mas como operacionalizar este fluxo informal de informações? Neste sentido, duas questões devem ser observadas: quem promove e controla a circulação dos dados, e que dados serão disponibilizados. No país, a Secretaria Nacional de Segurança Pública possui a função de fomentar a integração dos vários órgãos vinculados ao Subsistema de Inteligência de Segurança Pública e já coordena um sistema de troca de informações de inteligência, denominado Rede Nacional de Informações de Segurança Pública. Não obstante, estas trocas obedecem uma lógica formal, orientada pela doutrina que regula os pedidos de busca, a criação de Relints (relatórios de inteligência), condições de circulação etc, tratam-se de informações classificadas. Neste sentido, voltamos para o problema da agilidade. Torna-se crucial para o país o desenvolvimento de uma nova arquitetura de inteligência, na qual as agências compartilhem informações sensíveis, que seriam validadas e operacionalizadas, sob o regime de um protocolo único.

Segundo Bayer, um dos grandes problemas relacionados à troca de informações diz respeito à cultura ainda existente, de se classificar todo tipo de informações. É uma das faces mais visíveis da disputa de territórios empreendidas nos setores de inteligência, que ainda agem dentro da lógica de Guerra Fria. A informação classificada se torna inacessível a uma grande porcentagem de locais, nos quais seria extremamente necessária. Na perspectiva do autor, outro problema seria o fato de que, ao se classificar uma informação, desperta-se o interesse sobre a mesma, tornando-a objeto de desejo, o que lhe imprime maior vulnerabilidade.<sup>590</sup>

Na nova legislação brasileira encontramos em informações passíveis de classificação, aquelas cujo conhecimento público comprometeria as atividades de inteligência ou de investigação, relacionadas à prevenção ou repressão de infrações (Art. 23, Item VIII).<sup>591</sup> Mas como definir realisticamente quais informações, principalmente no ambiente criminal, deveriam ser classificadas, e quais não deveriam ter sua circulação restrita em relação aos vários órgãos que dela poderiam tirar proveito, para uma ação legítima? A proposta implementada por Bayer nos aponta alguns caminhos que promoveriam uma inversão da lógica tão difundida do período de Guerra Fria, inadequada para o enfrentamento dos complexos problemas impostos pela globalização da tecnologia de comunicação: não classificar informações, a menos que haja uma probabilidade concreta de este conhecimento causar danos à segurança nacional.<sup>592</sup> Ainda que o termo “segurança nacional” seja obscuro, o que o autor defende é que uma informação não deve ser classificada apenas porque desta forma: a) ocultaria uma violação à lei, um erro ou uma ineficiência administrativa; b) apenas visasse prevenir um constrangimento a uma pessoa, organização ou agência; c) impedisse a competição entre órgãos ou; d) prevenisse ou atrasasse a divulgação de uma informação que não requeira proteção, em interesse da segurança nacional.<sup>593</sup>

Ao denunciar a cultura da super-classificação das informações, que visa substancialmente esconder informações políticas constrangedoras e eliminá-las da esfera de competição interburocrática, Bayer atesta que apesar de a comunidade de inteligência recorrer a este procedimento com o discurso de se proteger fontes e métodos, e a comunidade policial invocar a classificação para a proteção de suas investigações, existem muitas ocasiões em que pode haver cooperação em torno de vários temas. “A classificação é tipicamente

uma decisão política, e não uma ação técnica”.<sup>594</sup> A saída seria substituir a classificação pela categorização de informação sensível. Por sua capacidade de auto-regulação, a troca de informações sensíveis estimularia, segundo o autor, uma transmissão mais segura do dado, uma vez que: a informação que circula sem classificação não seria objeto de cobiça como o é a informação classificada; há sempre a preocupação, por parte do próprio agente policial, de que ao se vazarem uma informação, corre-se o risco de “queimar” um caso pela libertação de qualquer informação sem autorização; e pelo fato de que as informações penais são claramente protegidas por lei e seu vazamento é considerado crime. É importante ficar atento ao fato de que cuidado com a circulação é diferente da eliminação da circulação da informação.<sup>595</sup> O uso dos critérios acima mencionados já fornecem dicas para a transformação da categorização das informações, de classificadas, para sensíveis.

Seria de extrema importância que a administração do Subsistema de Inteligência de Segurança Pública, sob responsabilidade da Secretaria Nacional de Segurança Pública, desenvolvesse cursos não apenas para a divulgação da Doutrina, engendrando um currículo mais padronizado para os profissionais de inteligência, mas que também fomentasse uma nova cultura de indexação da informação provendo, materialmente, os equipamentos e softwares necessários para viabilizar um acesso mais amplo aos vários bancos de dados existentes no país, capazes de contribuir com o tema da segurança pública. Tais cursos, compostos por membros das mais distintas organizações, não apenas promove a aproximação entre estes profissionais, como permite o desenvolvimento de confiança mútua, elemento fundamental para a troca de informação e na atuação pré-delitual.

### Diagnósticos e prognósticos

Em resumo, o que podemos dizer acerca do desenvolvimento de um sistema integrado de inteligência no país? No Brasil, as funções compreendidas na esfera da segurança interna (inteligência de segurança/doméstica e inteligência criminal/Law Enforcement intelligence), encontram-se imiscuídas na definição de Inteligência de Segurança Pública, o que é extremamente problemático, na medida em que apenas a atividade de inteligência desenvolvida no âmbito de uma investigação policial possui mandato para realizar a coleta intrusiva de dados.

## Gestão de Inteligência em las Américas

A padronização da linguagem e dos procedimentos também é de importância crucial para promover eficácia e legitimidade dentro do Subsistema de Inteligência de Segurança Pública, pois se o seu desenvolvimento depende de bons profissionais, é necessário um elemento balizador dos conceitos e valores que devem orientá-los. A utilização da Doutrina Nacional de Inteligência de Segurança Pública, aprovada pelo Conselho Especial em julho de 2009, ainda não compõe o universo de práticas implementadas pelo Subsistema de Inteligência de Segurança Pública. Primeiro, porque ainda não existe um interesse efetivo de interação, por parte das corporações envolvidas, que force a aplicação do “vocabulário” comum. O “dever ser” dos sistemas de inteligência permanece como um imperativo categórico muito aquém da nossa realidade. Nem mesmo no âmbito do executivo federal, a doutrina se implementa.<sup>596</sup> Este fator pode invalidar sua utilidade, já que não chega a quem precisa. Entre os sistemas estaduais, ainda inexistente um trabalho de cooperação ou interação institucionalizado, seja formal ou informal (redes sociais). Não há no país, em termos práticos, um entendimento padrão sobre os componentes fundamentais de inteligência de segurança pública, inviabilizando a definição das prioridades no desenvolvimento de ações políticas e uma administração de recursos conforme as orientações mais adequadas para o contexto democrático.

É claro que a padronização sobre os conceitos e técnicas utilizadas no âmbito da Inteligência de Segurança Pública não garante, por si só, a capilaridade do sistema. É preciso comprometimento, confiança, uma mudança na cultura de classificação das informações, bem como um órgão responsável por promover a integração do sistema, amparada pelos pressupostos da doutrina, capaz de fomentar a confiança entre seus componentes, para que os produtos realmente sejam produzidos de acordo com os padrões definidos, e para o que é mais importante, para que circulem de forma inteligível. Conforme pudemos averiguar em recente tendência internacional, a útil troca de informações sensíveis pode ocorrer tanto por meios formais, quanto informais (redes profissionais sociais), saber quem deve produzir informações, saber o que determinadas expressões significam, e haver uma confiança mínima entre as instituições, são requisitos mínimos para que a troca ocorra, independentemente dos meios.

Quanto à eficácia do Subsistema de Inteligência de Segurança Pública criado em 2000, não foi ainda, absolutamente, capaz de promover uma interação

satisfatória entre as distintas corporações. Entre os desafios identificados pelos gestores e operadores da atividade no período imediatamente posterior à sua criação,<sup>597</sup> a maioria ainda está presente: falta de mandatos, de capacitação, de gestão eficiente, de padronização, cooperação. Apenas dois, dos poucos problemas inicialmente identificados, foram sanados: a aprovação de uma nova doutrina, e a criação de uma rede interna, capaz de promover a transmissão segura de informações classificadas. O sistema Rede Nacional de Informações de Segurança Pública foi criado com o intuito de atender esta demanda, não obstante, ainda não é um recurso amplamente utilizado. Na medida em que a falta de confiança e de cooperação entre distintos órgãos ainda imperam, as soluções informais/pessoais, não institucionalizadas, são vistas como a melhor opção.

Ou seja, apesar de o discurso sobre a necessidade de se produzir mais e melhores informações sobre os crimes e os criminosos no país ser moeda corrente, ainda não alcançamos na área de segurança pública um grau de especialização e proeminência capaz de gerar o que em outros países já se chama de policiamento liderado pela inteligência (*intelligence-led policing*).<sup>598</sup> Uma prioridade seria então, precisamente, construirmos no país uma cultura capaz de perceber as respostas e os resultados operacionais imediatos desta integração. A produção do conhecimento no trabalho policial, e mesmo no sistema criminal, em seu sentido amplo, depende fundamentalmente da sinergia produzida entre os ganhos tecnológicos viabilizados pela infra-estrutura de Tecnologia de Informações e Comunicações, pela qualidade dos bancos de dados, e pela riqueza de informações entranhadas na própria atividade operacional (preventiva e investigativa).

O desenvolvimento de um sistema de inteligência de segurança pública no Brasil ainda demanda valorização da atividade por parte dos gestores da segurança pública, conhecimento sobre suas funções, fomento à sua integração, cooperação, capacitação e, sobretudo, humildade aos gestores para conservarem os avanços anteriormente alcançados. Se administrar a inteligência depende do desenvolvimento de um arcabouço capaz de conduzi-la, como um gestor conseguirá definir seus componentes essenciais e definir os recursos técnicos e profissionais necessários, se não compreende e valoriza a atividade? Como será possível fomentar capacitação, integração, propor reformas, melhoria em sua regulamentação, sem o estabelecimento claro sobre suas esferas de atuação?

## Gestão de Inteligência em las Américas

Tal desconhecimento inviabiliza uma condução efetiva da atividade, que vai além da sua administração. Administrar um subsistema de inteligência de segurança pública, o que tem sido feito, apesar dos vários altos e baixos, é muito distinto de conduzir uma política de inteligência, nossa demanda efetiva. Sem o atendimento deste requisito, os graus de governabilidade do sistema continuarão seriamente comprometidos.

Urge no Brasil a revisão dos mecanismos legais que regulamentem a coleta de informações tanto por parte das polícias quanto da chamada inteligência de Estado. A ABIN, por exemplo, não possui mandato para interceptar comunicações de qualquer tipo. Se a atividade de inteligência lida com conflito de vontades e serve para obter informações que são protegidas e/ou negadas, o que justificaria a existência de um órgão de inteligência (nesse caso, no mais alto nível de condução do Estado), sem este tipo de mandato executivo para o exercício da inteligência e contra-inteligência? Fica a pergunta, apresento algumas respostas:

Quadro síntese:

Tabela 15 Esquema de Sugestões para o melhoramento da Inteligência Nacional		
Critério de Eficácia	Situação Atual	Propostas
Definição clara do Conceito de Inteligência de Segurança Pública: deve ser amplamente compreendido e legitimado por aqueles que dela se servem.	Ambigüidade conceitual	Especificar as áreas relevantes de atuação (Defesa, Segurança Pública e Relações Internacionais), delimitando a área de atuação de cada um dos componentes da comunidade de inteligência.
Definir quem governa, quem gerencia, quem executa, como se governa.	Ambigüidade sobre os papéis atribuídos a civis, militares e policiais no processo de produção do conhecimento: ameaça à privacidade e outros direitos civis	Definir a atribuição de cada um dos órgãos dentro do sistema, considerando sua natureza, local dentro do subsistema e, principalmente, sua atividade fim.

Tabela 15, (continua)		
Esquema de Sugestões para o melhoramento da Inteligência Nacional		
Critério de Eficácia	Situação Atual	Propostas
Definir como se governa: planejar, capacitar, avaliar e valorizar profissionais da área.	Pendência na aprovação da Política Nacional de Inteligência	Aprovação da Política, que orientará os Planos e metas para cada uma das respectivas áreas, de acordo com os objetivos políticos do governo.
Padronização	Pendência na divulgação da Doutrina Nacional de Inteligência de Segurança Pública	Promoção de encontros e cursos que promovam aproximação entre componentes e padronização de linguagem.
Cooperação	Corporativismo Conservador	Promoção de processos de integração, capazes de gerar uma leitura positiva do corporativismo, que promova sentimento de pertencimento, desapego à propriedade da informação e preocupação com a atividade fim: manutenção da ordem pública e preservação dos Estado de Direito.
Gestão eficiente	Não corrigem erros, porque não os detectam, falta interlocução entre as “castas”.	Quebrar o abismo existente entre operadores de inteligência (que sabem muito) e gestores, com os quais pouco dialogam.
Compartilhamento de informações	Guarda corporativa ou privada da informação	a) Institucionalização dos procedimentos informais de coleta e manuseio de dados, por meio da aproximação entre colegas. (Poderia ser promovido

Tabela 15, (continua)		
Esquema de Sugestões para o melhoramento da Inteligência Nacional		
Critério de Eficácia	Situação Atual	Propostas
		pela Secretaria Nacional de Segurança Pública, por meio de Protocolo Seguro). b) Fomento da cultura de compartilhamento, em detrimento da de compartimentação.

Fonte: Compilado pela autora.

### Biografia da autora

**Priscila Brandão** é doutora em Ciências Sociais pela Universidade Estadual de Campinas (2005), Pós-Doutora em Governança e Governabilidade no Combate ao Narcotráfico (National Defense University/2010) e atualmente desenvolve pós-doutorado pela Universidade de Burgos/Espanha, sobre profissionalização na área de inteligência. Desde janeiro de 2006 é professora adjunta da Universidade Federal de Minas Gerais. Possui experiência na área de História, com ênfase em História das Instituições Políticas Contemporâneas, atuando principalmente nos temas sobre ditadura militar, comunidade de inteligência, Abin, América Latina e Inteligência Criminal. Desenvolve pesquisa sobre a implementação do Subsistema Brasileiro de Inteligência de Segurança Pública/SISP e do sistema de inteligência do Departamento de Polícia Federal, do Ministério da Justiça (DPF-MJ). É consultora dos governos Federal e de alguns governos estaduais, para a área de inteligência criminal. É líder do Diretório de Pesquisa do Conselho Nacional de Desenvolvimento Científico e Tecnológico: Inteligência Governamental; e coordenadora do Centro de Estudos Estratégicos e Inteligência Governamental da UFMG. Autora de *SNI e ABIN*. Rio de Janeiro, EDFGV, 2002; *Serviços Secretos e Democracia*, Niterói, Editora Impetus, 2010 e vários outros artigos sobre o tema. Ver currículo completo em: <http://lattes.cnpq.br/5546418263728807>.





## Inteligencia en el Ámbito Penitenciario: Condiciones para su Relación con la Seguridad Pública

Liza Zúñiga Collado

### Introducción

¿Por qué es deseable el desarrollo de tareas de inteligencia estratégica en el ámbito carcelario? ¿Por qué tendría valor estratégico? ¿Cómo se puede lograr la gestión de la función de inteligencia en este ámbito? Éstas son las preguntas que guían el presente artículo, en el cual se presenta un acercamiento a dos áreas que parecen no juntarse, pero que tienen una relación debido a la inserción de la inteligencia en la seguridad pública. No existen estudios ni del ámbito penitenciario ni desde la inteligencia que aborden esto, que se podría considerar un nuevo ámbito de aplicación de la inteligencia, por lo tanto, las ideas aquí planteadas se presentan a modo de reflexión y desafío pendiente. La revisión de diferentes casos en América Latina, desde la normativa, orientará esta discusión y mostrará que los espacios están abiertos en algunos casos, aunque lejos de concretar la inserción del sistema carcelario en la función de inteligencia.

Para responder a las preguntas planteadas, se comienza con una justificación teórica basada en el concepto de reformas del sector seguridad que se desarrolló en la década de los noventa y del cual se tomará la idea de *sistema de seguridad*, pues otorga la posibilidad de desarrollar una red de organismos que colaboren entre sí, respetando los ámbitos de competencia de cada uno, pero asegurando un nivel de coordinación mínimo que permita el desarrollo del sector y de cada institución de forma complementaria. Bajo este marco conceptual se plantea la necesidad de incluir al sistema penitenciario en las labores de inteligencia, con el objetivo de que no sea un mero receptor de decisiones judiciales y políticas criminales, sino que tenga un rol activo en el sistema de seguridad estatal.

Para sustentar la discusión, en el segundo punto se presenta la conformación de las agencias de inteligencia en América Latina, señalando la presencia de leyes, definiciones y organismos que la componen. En ello se aprecian dos grupos de países: aquellos que han logrado avanzar hacia leyes de inteligencia

con sistemas, que con más o menos elementos constituyen un sistema de inteligencia que contempla definiciones, principios de actuación, límites y controles a la labor de inteligencia y una red de organismos que en distintos ámbitos colaboran a ese fin; en tanto, un segundo grupo de países muestra un escaso o nulo desarrollo en este ámbito. Lo que une a ambos grupos es que perdura, de manera general, una concepción tradicional de inteligencia basada en la inteligencia estratégica, la militar y la policial.

Con lo anterior en vista, el tercer y último punto presenta las condiciones que debieran darse para que la inteligencia abarque también el ámbito penitenciario, pues más allá de que la jurisprudencia o una política pública lo indiquen, lo cierto es que el sistema carcelario de América Latina arrastra una crisis que, en las condiciones actuales, hace imposible -o muy difícil- la implementación de servicios de inteligencia en el sector, o incluso la consideración de ella. No obstante, es una tarea necesaria que ayudaría a mejorar la administración de las cárceles e integrar al sistema de seguridad a una institución largamente postergada. Es cierto que pensar en servicios de inteligencia en el sector carcelario es ambicioso debido a la situación carcelaria de la región, pero es factible desarrollarla en la medida de lo posible y en cuanto el sistema comience al mismo tiempo a superar sus múltiples deficiencias.

### **Sistema de seguridad: cooperación para la seguridad multidimensional**

Si bien la idea de sector seguridad como un todo nació en la década de los noventa en el contexto de los países de Europa del Este que debían reorganizar y, por tanto, reformar sus instituciones de seguridad, es igualmente aplicable a otros contextos, como países en vías de desarrollo o desarrollados, que bajo este concepto pueden perfeccionar sus instituciones de seguridad. En América Latina, el contexto de reconfiguración política no fue el mismo que en Europa del Este, por el tipo de conflicto vivido, pero sí hubo en la misma década una serie de reformas post dictaduras militares, en la era de la llamada “tercera ola de democratización”. La mayoría de estas reformas estuvieron centradas en restablecer o reconfigurar el liderazgo civil y político sobre las fuerzas armadas, así como separar la acción policial de la militar y hacer de estas instituciones cuerpos obedientes y no deliberantes.<sup>599</sup> Pero en este proceso de reforma inicial no se consideraron otros actores del sector, especialmente

## Gestión de Inteligencia en las Américas

del área de justicia. Así, los servicios carcelarios no fueron integrados y en las dos últimas décadas fueron el recipiente de políticas criminales cada vez más punitivas, con penas de mayor duración y nuevos delitos, pero sin un contrapeso de política penitenciaria que se encargara de las cárceles. En consecuencia, los recintos de privación de libertad continuaron recibiendo cada vez más reclusos sin mayores modificaciones en el personal, en la infraestructura y en los programas disponibles para una población penal más numerosa y con características diferentes, en algunos casos más violenta y organizada. La situación descrita está presente, con matices, en toda América Latina.

Pero, ¿por qué incluir a los servicios carcelarios en el sistema de seguridad? De acuerdo al concepto amplio de seguridad de la Organización para la Cooperación y el Desarrollo Económico (OCDE) “La seguridad del pueblo y la seguridad de los Estados son mutuamente reforzantes. Una amplia gama de instituciones del Estado y otras entidades pueden ser responsables de asegurar aspectos de seguridad”. Dentro de este concepto amplio, la OCDE define al *sector seguridad* como

término usado para describir un sistema de seguridad que incluya a todos los actores, sus roles, responsabilidades y acciones, trabajando en conjunto para administrar y operar el sistema de una forma congruente con las normas democráticas y principios de buen gobierno. De esta forma contribuye al buen funcionamiento del marco de la seguridad.<sup>600</sup>

De esta definición se desprenden dos elementos que justifican la incorporación de las cárceles en el sector. El primero es que se incluye a *todos los actores*, ya sean centrales (como las fuerzas armadas, las policías, los servicios de inteligencia y similares), administrativos y de control (ministerios, comisiones legislativas, administración financiera), de justicia (instituciones penales, cortes, comisiones de derechos humanos) y fuerzas no estatales (como los servicios de seguridad privada). En este sentido el sistema carcelario forma parte del sector aunque no sea un actor central en sentido de las instituciones armadas. El segundo, es que el sistema debe contribuir al *buen gobierno* y al funcionamiento del sector. Esto es, fomentar la gobernabilidad, dado que la seguridad es una de las bases fundamentales que permiten el desarrollo de las personas.

Respecto del concepto de gobernabilidad en el ámbito de la seguridad, se destaca aquí el adoptado por la Comisión Interamericana de Derechos Humanos, que señala lo siguiente: la gobernabilidad democrática de la seguridad ciudadana es la capacidad institucional por parte de las autoridades legítimas de diseñar, implementar y evaluar políticas de prevención y control de la violencia y el delito.<sup>601</sup> De ella es necesario destacar tres de sus componentes: (i) se refiere a la gobernabilidad en un sistema democrático, es decir, donde existen -básicamente- autoridades civiles electas por la ciudadanía en procesos libres; (ii) apunta a la idea de seguridad ciudadana, es decir, aquélla que va más allá de las instituciones armadas tradicionales (como la policía) e implica a la ciudadanía, es decir, un concepto más integral de la seguridad; y (iii) implica medidas tanto preventivas, como de control. Esto último es especialmente importante en el ámbito penitenciario, pues si bien forma parte del sistema penal y, por ende, su enfoque está en el control de quien ha quebrantado la ley, también es susceptible de políticas preventivas, que apunten esencialmente a disminuir la reincidencia.

Si bien América Latina ha avanzado en políticas de seguridad ciudadana con participación comunitaria, en programas de prevención de todo tipo y en determinadas reformas ministeriales y policiales, las cárceles han permanecido casi intactas, sin políticas penitenciarias, con escasos resultados positivos que responden más bien a programas y esfuerzos aislados. Esto ha sucedido por una parte, porque tradicionalmente las policías y el poder judicial no han visto a la administración penitenciaria como un igual en el sistema de justicia criminal, perpetuando la idea de que el personal penitenciario es sólo personal de custodia y no de justicia;<sup>602</sup> y, por otra parte, porque no es políticamente rentable para los gobiernos demostrar que son capaces de desarrollar un sistema carcelario en el marco del respeto a los derechos humanos, por el contrario, los tomadores de decisiones han creído que enviar más personas a la cárcel -sin importar lo que allí adentro suceda- es la mejor manera de responder a las demandas ciudadanas por mayor seguridad, conocido como populismo punitivo.<sup>603</sup>

Como contraparte se ha instalado en América Latina, al menos discursivamente, la idea de seguridad humana y luego, la de seguridad multidimensional, que concuerdan con la mirada de sistema para el conjunto de las instituciones de seguridad. El origen de esta conceptualización de la seguridad como un

## Gestión de Inteligencia en las Américas

fenómeno multidimensional se remonta en la OEA a la Declaración sobre Seguridad de las Américas del año 2003, cuyo enfoque sostiene que la

seguridad en el Hemisferio es de alcance multidimensional, incluye las amenazas tradicionales y las nuevas amenazas, preocupaciones y otros desafíos a la seguridad de los Estados del Hemisferio, incorpora las prioridades de cada Estado, contribuye a la consolidación de la paz, al desarrollo integral y a la justicia social, y se basa en valores democráticos, el respeto, la promoción y defensa de los derechos humanos, la solidaridad, la cooperación y el respeto a la soberanía nacional.<sup>604</sup>

Este nuevo concepto es semejante a la idea de seguridad humana -impulsada por el PNUD y en particular por los gobiernos de Canadá y Japón a principios de la década del noventa- de la cual se ha destacado positivamente su enfoque en las personas y su naturaleza integradora, así como su carácter multidimensional y su acento en el multilateralismo y la cooperación, aunque al mismo tiempo su campo de acción resulta muy amplio e introduce la dimensión seguridad en otras áreas del desarrollo.<sup>605</sup>

En consecuencia, si la seguridad tiene dimensiones múltiples, porque diversos son los orígenes de las amenazas, también deben ser múltiples los organismos encargados de hacerles frente, en el entendido de que no es posible descansar en la labor de una o dos instituciones. En este sentido, el rol de las cárceles es fundamental en el control de la delincuencia común y organizada, pudiendo desarrollar inteligencia en su ámbito de acción, pero también estando facultados para colaborar con los órganos centrales. De esa forma pueden contribuir a una mejor gestión de los organismos carcelarios, colaborando en el proceso decisional y en el uso óptimo de la información con que cuentan las instituciones carcelarias que resulta esencial para la seguridad institucional y pública. Con ello las administraciones penitenciarias pueden mejorar su propia seguridad y ser un aporte para el resto, permitiéndoles pasar también de un rol pasivo a uno más activo en el sistema de seguridad.

### Función de inteligencia y función penitenciaria

La inteligencia estratégica es una labor diseñada para proveer de un panorama que se requiere para planificar el futuro, es decir, se trata de información

clave para la toma de decisiones. El proceso de producción de inteligencia requiere de planificación, desarrollo de sistemas y métodos para recolectar información y, finalmente, hacer análisis y administrar la organización. Según estos principios es un proceso que puede ser aplicado a muchas áreas, pero la inteligencia estratégica estuvo por mucho tiempo concentrada en el ámbito de la defensa nacional. Sin embargo, hoy incluso el ámbito empresarial aplica este concepto y, en materia de asuntos públicos, la comunidad de inteligencia también debe tomar en su accionar cuestiones económicas y sociales.

Entre las cuestiones sociales, resulta evidente que la delincuencia es un área donde se puede y se debe realizar un análisis de inteligencia que permita planificar las estrategias para enfrentar un fenómeno cambiante. El análisis de inteligencia en materias de seguridad pública permitiría una mejor planificación de las estrategias, tanto policiales como de prevención social, frente a una delincuencia que cambia y busca permanentemente nuevas formas de cometer delitos, asimismo permitirá tomar decisiones con más y mejor información para el mantenimiento del orden público. En Estados Unidos, por ejemplo, entre la década de los 50 y los 60 se hizo necesaria la labor de inteligencia penitenciaria para monitorear el movimiento de las pandillas dentro de las cárceles que estaban desafiando al sistema, y a poco a poco se fueron desarrollando grupos especiales para esta labor con personal dedicado y entrenado para ello.<sup>606</sup> El actual nivel de coordinación de la delincuencia organizada dentro de las cárceles y de pandillas -esto último especialmente en Centroamérica- es una señal de que la inteligencia se está haciendo cada vez más necesaria en las cárceles.

La inteligencia policial es un área asumida por la mayoría de las policías latinoamericanas, ya sea por medio de unidades de prevención o departamentos de inteligencia policial, o indirectamente en departamentos de investigación criminal. Sin embargo, las administraciones carcelarias no han incorporado la inteligencia entre sus labores, limitándose a la custodia de los reclusos y en menor medida, a los programas de reinserción. Se trata además, de un área en la que a falta de investigación empírica, se suelen hacer generalizaciones basadas en reportes de prensa, por lo que puede haber una distancia considerable entre la realidad y el imaginario social respecto de las cárceles. El problema es cuando ese imaginario está presente también en los tomadores de decisiones,

## Gestión de Inteligencia en las Américas

por ello es necesaria la inteligencia carcelaria y la investigación empírica sobre las características de la población penal.

¿Por qué la inteligencia debería ser aplicada al ámbito carcelario? Principalmente por dos razones. La primera porque, como se ha señalado, se trata de un actor del sistema de seguridad, por lo tanto, para que este sistema sea gobernable en su conjunto y eficaz en su implementación, es necesaria la coordinación entre actores. En este sentido, la administración penitenciaria tiene mucho que aportar desde su labor de custodia de la población privada de libertad, por las dinámicas que se generan dentro de la cárcel que ilustran las relaciones de poder, inequidad, orden y conflicto.<sup>607</sup> El personal de custodia es ojos y oídos de analistas de inteligencia, pues debido al contacto diario con los reclusos pueden proveer de información relevante.<sup>608</sup> Además, la cárcel es el símbolo más potente del poder del Estado para castigar, pero al mismo tiempo muestra las fallas de éste para integrar a todos los ciudadanos en un sistema de normas. Esto hace que sea indispensable considerarla dentro del sistema de instituciones de seguridad, porque es un elemento que puede revelar aspectos sociales que, a su vez, permitan el perfeccionamiento gradual de políticas públicas orientadas a los grupos envueltos en la delincuencia.

La segunda razón radica en que el desarrollo de inteligencia en el ámbito penitenciario le será útil a la propia administración del sistema carcelario para planificar su accionar futuro, para realizar cambios en su política y anticiparse a hechos que amenacen la seguridad interna, como los motines e intentos de escape. Para esto, es vital que el personal penitenciario tenga el entrenamiento adecuado y conozca el movimiento de los reclusos. Los arreglos informales entre ambos grupos son, sin duda, una fuente de información que tiene además efectos en el orden de los recintos carcelarios: alivian las tensiones y déficits del sistema, mantiene bajo control a los prisioneros más conflictivos y refuerza el estatus de los reclusos líderes.<sup>609</sup> La inteligencia como proceso sistemático de recolección, evaluación y análisis de información, es aplicable al ámbito carcelario, donde las decisiones que se tomen tienen directa influencia en la seguridad de las personas -reclusos y funcionarios- por lo cual requiere de un reconocimiento. Su responsabilidad puede recaer en monitorear, identificar y documentar miembros de pandillas o de organizaciones criminales coordinándose con agentes externos, como policías y oficiales de justicia.



## Legislación de inteligencia y la oportunidad para un sistema integrado de seguridad

Tanto la defensa, como protección de amenazas externas, el orden y la seguridad interna y la provisión de justicia son tareas exclusivas del Estado por tener el monopolio del uso de la fuerza; por lo tanto, todas ellas deben ser el primer círculo de un sistema de inteligencia. El poder judicial puede tener un rol de control, decidiendo, por ejemplo, sobre el uso de determinados medios de recolección de información. Pero organismos que dependen de él también pueden *hacer* inteligencia, como los sistemas penitenciarios. La consideración del poder judicial como órgano de supervisión y control de la inteligencia solamente ha sido recogida por aquellos países que tienen una legislación específica en materia de inteligencia.<sup>610</sup>

Varios países de la región han desarrollado una legislación sobre inteligencia nacional (véase Tabla 3). Algunas son más completas que otras e incluyen definiciones básicas, actores del sistema, roles y mecanismos de control (véase Tabla 4). En otros casos hay decretos que constituyen un organismo, pero señalan muy poco sobre otros aspectos (como en El Salvador).

En el caso de Argentina, dice la Ley de Inteligencia (Art. 13 de Ley 25520, del 2001) que la Secretaría de Inteligencia puede “Requerir a todos los órganos de la Administración Pública Nacional la información necesaria para el cumplimiento de sus funciones”. Ahí vemos una oportunidad para un intercambio de información e inteligencia entre oficiales del sistema penitenciario y el sistema nacional de inteligencia de la nación. A la distancia de casi una década, se señalan entre las funciones del Ministerio de Seguridad de la Nación (creado en 2010) “entender en la producción de inteligencia e información que compete a las Fuerzas de Seguridad y las Fuerzas Policiales”,<sup>611</sup> es decir, tiene un rol de inteligencia en cuanto las policías que este Ministerio coordina realizan tal labor. Hay mención de inteligencia penitenciaria del Servicio Penitenciario Federal en la ley argentina 27126 de 2015, que transfiere a la nueva Agencia Federal de Inteligencia las competencias y el personal que se requiera de la Dirección Nacional de Inteligencia Criminal.

En el caso de Chile, la ley que crea la Agencia Nacional de Inteligencia (ANI) tampoco señala la participación de Gendarmería (el organismo encargado de la administración y custodia de las cárceles) entre las instituciones que forman

## Gestión de Inteligencia en las Américas

parte del sistema de inteligencia. Similar al caso argentino, contempla la inteligencia militar, la estratégica y la criminal, esta última entregada a las fuerzas de orden y seguridad, es decir, las policías; aunque señala que la ANI puede requerir de la Dirección Nacional de Gendarmería la información que sea de su ámbito de responsabilidad y que se relacione con la competencia de la ANI, ante lo cual Gendarmería está obligada a otorgar información. En este caso, la inteligencia criminal, entendida como policial “Comprende el procesamiento de la información relacionada con las actividades de personas, grupos y organizaciones que de cualquier manera afecten o puedan afectar las condiciones del orden público y de la seguridad pública interior” (Ley 19972, Art. 22). Estas organizaciones o grupos siguen en muchos casos funcionando desde las cárceles, por lo cual es necesario que Gendarmería forme parte de este sistema de manera más directa y no sólo cuando la ANI lo requiera. Si Gendarmería realizara de manera permanente inteligencia e institucionalizara esta labor, podría ser un aporte sustantivo al sistema. En efecto, se hace especial mención a ésta en la ley citada, reconociendo su importancia.

En Brasil, el principal órgano que es la Agencia Brasileña de Inteligencia (ABIN), depende de la Presidencia de la República y tiene como fin “planear, ejecutar, coordinar, supervisar y controlar las actividades de inteligencia del país” (Ley 9833, Art. 3). La ley señala que serán parte del sistema de inteligencia los órganos de administración pública federal que directa o indirectamente pueda producir conocimientos de interés para las actividades de inteligencia, en especial los responsables por la defensa externa, la seguridad interna y las relaciones exteriores (Ley 9833 de 1999, Art. 2). Esto deja la puerta abierta para que el Departamento Penitenciario Nacional, del Ministerio de Justicia, eventualmente, forme parte de este sistema. Luego, mediante el Decreto No. 3695 del 21/12/2000, el gobierno brasileño creó el Subsistema de Inteligencia de Seguridad Pública, integrado por los Ministros de Justicia (Interior), Hacienda, Defensa e Integración Nacional, y el Gabinete de Seguridad Institucional de la Presidencia. Esta nueva organización es dirigida por la Secretaría Nacional de Seguridad Pública del Ministerio de Justicia. El órgano ejecutivo es el Consejo Especial del Subsistema de Inteligencia de Seguridad Pública, en el que participan: el secretario nacional de seguridad pública -quien lo preside-; un representante del órgano de inteligencia del Departamento de Policía Federal y otro de la Policía Rodoviaria; dos representantes del ministerio de Hacienda; dos del Ministerio de Defensa; uno

del Gabinete de Seguridad Institucional de la Presidencia; uno de la Defensa Civil y uno de la ABIN. Como se aprecia, no hay ningún representante del Departamento Penitenciario.

En el caso de Perú, la Dirección General de Inteligencia del Ministerio del Interior (DIGIMIN) es la encargada de coordinar y centralizar la inteligencia relacionada al orden interno, la seguridad pública, el crimen organizado y las nuevas amenazas transnacionales. Si bien la ley menciona un “campo no militar” donde se incluyen los asuntos políticos, económicos y sociales, no se menciona como parte del sistema al Ministerio de Justicia ni al Instituto Nacional Penitenciario.

En Guatemala, por medio de los Acuerdos de Paz de 1996, se limitó el accionar de la Dirección de Inteligencia del Ejército al ámbito de la defensa. De ese modo la Dirección General de Inteligencia Civil (DIGICI) como órgano civil, queda encargada de la inteligencia para proteger del crimen organizado y delincuencia común, y a los intereses políticos, económicos, sociales, industriales, comerciales, tecnológicos y estratégicos del país, es decir, su accionar está en muchos ámbitos internos, entre ellos, incluye la inteligencia criminal. Al depender de la misma cartera que la Policía Nacional Civil y la Dirección General de Centros Penales y estar en la misma línea de dependencia directa del Ministro de Gobernación, se puede suponer un nivel de coordinación. De hecho, entre las funciones de la DIGICI está “recabar y centralizar la información proveniente de las dependencias del Ministerio de Gobernación”, que incluiría el Sistema Penitenciario. Pero hasta la fecha no se menciona en ningún documento un rol particular para ninguna de ellas.

El Jefe de Estado de Ecuador, Rafael Correa, señala en 2009 (Acuerdo Ministerial 026) que el Sistema Nacional de Inteligencia (SNI) operará con base en el nuevo Plan Nacional de Inteligencia.<sup>612</sup> El Acuerdo indica que la Secretaría de Inteligencia es el órgano rector del Sistema Nacional de Inteligencia que planifica, norma y coordina la búsqueda, procesamiento y producción de Inteligencia. Este sistema está compuesto por el Subsistema de Inteligencia Militar, para la defensa nacional, el Subsistema de Inteligencia Policial, para la protección interna y la Unidad de Gestión de Seguridad Interna de la Presidencia de la República. Señala además que participarán “otros organismos de inteligencia que se crearen o adscribieren en el futuro” y “otras instituciones y organismos que posean o produzcan información de interés para los fines

## Gestión de Inteligencia en las Américas

de la conducción y seguridad integral del Estado”. En definitiva, tampoco considera la inteligencia penitenciaria, aunque deja abierta la posibilidad de que se creen nuevos organismos que formen parte del sistema, pero por el momento se basa en la inteligencia militar, policial y un organismo civil que coordina.

En 2011, Colombia inicia el proyecto de Ley Estatutaria N° 195, que regula los organismos de inteligencia y contrainteligencia. Fue creado para superar el vacío legal dejado por la derogación de la ley 1288, del 2009. Impulsado por el poder ejecutivo desde el Ministerio de Defensa, el Proyecto considera definiciones, límites, fines, funciones y principios que regulan la actividad de inteligencia y contrainteligencia. Si bien existe el concepto de “comunidad de inteligencia” presente en la ley, no hay un organismo coordinador de carácter civil que centralice la actividad. Para esta labor de coordinación se ha conformado la Junta de Inteligencia Conjunta (JIC) que se reúne regularmente para analizar los asuntos relacionados con la seguridad y defensa del Estado, coordinar las actividades de inteligencia y contrainteligencia, y asegurar la cooperación entre los distintos organismos que las llevan a cabo. Esta Junta está conformada por el Ministro de la Defensa Nacional, Alto Asesor para la Seguridad Nacional, Viceministro de Defensa Nacional, el Jefe de Inteligencia Conjunta (en representación del Comandante General de las Fuerzas), los Jefes de Inteligencia del Ejército, la Armada y la Fuerza Aérea, el Director de Inteligencia Policial, el Director de la Unidad de Información y Análisis Financiero (UIAF) y el “Director de cualquier otro organismo de inteligencia y contrainteligencia facultado por Ley para llevar a cabo tales actividades”. Se señala también que las entidades públicas y privadas podrán cooperar con los organismos de inteligencia y contrainteligencia y que en caso de que la información solicitada esté amparada por la reserva legal, los organismos de inteligencia y las entidades públicas y privadas podrán suscribir convenios interinstitucionales de mutuo acuerdo para lograr los intercambios. En definitiva, tampoco incluye al sistema penitenciario, aunque deja abierta la puerta para que se incluyan otros organismos.

De los demás países, Nicaragua no tiene una ley de inteligencia ni un concepto de sistema y la Dirección de Información para la Defensa es un órgano del Ejército, no del Ministerio. Como señalan el artículo 51 del Decreto 25 (del 2007) -que reforma el Reglamento de la Ley de Organización, Competencia y Procedimientos del Poder Ejecutivo- y el artículo 26 del Código de

Organización, Jurisdicción y Previsión Social Militar (Ley 181 del 1994), “la Dirección de Información para la Defensa está destinada a obtener, procesar y analizar la información de actividades que atenten contra la soberanía, la integridad territorial de la nación y el orden constitucional. En ningún caso podrá realizar actividades de inteligencia política y se subordinará al Presidente de la República en su carácter de Jefe Supremo de la Fuerza de Defensa y Seguridad”. Por su parte, la Dirección de Contra Inteligencia Militar “es un organismo militar especializado, que está designado para la protección de la Institución, para la prevención de actividades delictivas y de acciones que se den a lo interno de la Institución que atenten contra la integridad de la misma”. También está destinada para garantizar la protección física de los mandos, de las instalaciones militares y de los bienes y recursos del Ejército (Ley 181, Art. 27).

En este caso la inteligencia está restringida al ámbito militar y de la defensa, pues aún cuando en 1993 se creó una Dirección de Asuntos de Inteligencia -como órgano civil, dependiente de la Presidencia- está conformado por tres subdirectores de la misma órbita militar y policial: un representante del Ministerio de Gobernación, otro de la Policía Nacional y un tercero de la Dirección de Información para la Defensa. Si bien la ley determina que puede ampliarse el número de subdirectores y entre sus materias figuran principalmente delitos como el tráfico y contrabando de diversas especies, no contempla por el momento la participación de otros organismos como el Sistema Penitenciario Nacional. En este caso la Policía Nacional Civil (PNC) y el Sistema Penitenciario Nacional dependen del mismo Ministerio de Gobernación, pero no hay una instancia formal donde se coordinen. La PNC por su parte tiene una unidad de inteligencia policial dentro de las llamadas “especialidades nacionales”, dependiendo directamente de la Dirección Nacional, sin embargo, la definición de sus funciones no aparece en la Ley de Policía Nacional.

En Costa Rica tampoco existe una ley de inteligencia. Es la ley que regula las fuerzas policiales (del 1994) la que determina la existencia de la Dirección de Inteligencia y Seguridad Nacional (DIS), como órgano informativo del Presidente de la República en materia de seguridad nacional. Funciona bajo el mando exclusivo del Presidente de la República, quien podrá delegar, en el Ministerio de la Presidencia, la supervisión del cumplimiento de las funciones de este cuerpo policial. Sin embargo, lo que figura en el organigrama policial no es la DIS, sino el Departamento de Inteligencia Policial está inserto en la

## Gestión de Inteligencia en las Américas

Dirección de Operaciones de la Policía. Al no tener fuerzas armadas esta es la única instancia de inteligencia con la que cuenta. Pero la ley no señala los ámbitos de aplicación, sólo señala que su función es “detectar, investigar, analizar y comunicar al Presidente de la República o al Ministro de la Presidencia, la información necesaria para prevenir hechos que impliquen riesgo para la independencia o la integridad territorial o pongan en peligro la estabilidad del país y de sus instituciones”. Sin embargo, a raíz de un escándalo sobre uso de información para extorsión por parte de la DIS, en febrero de 2011 se presentó un proyecto de ley para derogar esta dirección.<sup>613</sup>

En Honduras, que tampoco cuenta con una ley de inteligencia, tampoco existe un organismo que regule y controle las actividades de inteligencia a nivel estatal siendo la Dirección de Información Estratégica del Estado Mayor Conjunto de las Fuerzas Armadas la encargada de satisfacer la mayoría de los requerimientos de información e inteligencia ordenados por el gobierno. Además, la Policía Nacional tiene un área de inteligencia, pero no se menciona un posible rol del sistema penitenciario, aunque depende de la misma policía.

En Bolivia, que tampoco tiene una ley de inteligencia o una agencia rectora del sistema, los organismos que realizan inteligencia de manera independiente están en el ámbito militar, policial y político, este último por la Dirección Nacional de Inteligencia del Estado del Ministerio de Gobierno. No obstante, hay una preocupación por parte de la autoridad política con respecto a regular esta función a través de una ley, habiendo ingresado un proyecto de ley sobre la materia en el congreso. Dicho proyecto señala que el gobierno centralizará las labores de inteligencia con la creación de una Dirección de Inteligencia del Estado Plurinacional (DIDEP). Además del trabajo realizado tradicionalmente por militares y policías, la DIDEP contará con el aporte de cinco ministerios para la llamada “inteligencia estratégica”, que se nutrirá con la información ofrecida por los despachos de Relaciones Exteriores, Economía, Autonomía, Planificación del Desarrollo y el de Lucha Contra la Corrupción. Se menciona, en otros asuntos, que tendrá dos controles, el interno, a cargo de la Asamblea Plurinacional, y uno externo, por el Consejo Supremo de Defensa, pero sobre el sistema carcelario como posible colaborador, no se pronuncia.<sup>614</sup>

En Uruguay, luego de diversos cuestionamientos al accionar del coordinador de inteligencia del Estado, y de que el propio poder ejecutivo enviara un

proyecto de ley de inteligencia,<sup>615</sup> finalmente el 23 de noviembre de 2011 se votó en la Asamblea General la creación de una comisión especial que se dedique a la redacción de una ley nacional de inteligencia.<sup>616</sup>

Uruguay y Costa Rica son dos países donde la actual institucionalidad está en discusión, aunque aún no ha sido modificada, pero el hecho de que se comience a discutir -aunque sea a partir de escándalos por el mal o incorrecto uso de la información- es positivo, pues otorga la oportunidad de mejorar los mecanismos de coordinación y el control de sector. Estos debates son fundamentales, pues un problema central respecto de la democracia y su relación con la inteligencia es el limitado acceso a la información: la información de inteligencia existe pero su acceso está “limitado a quienes controlan directamente el sistema, excluyendo al público general, a la academia y, a menudo, a los representantes democráticamente elegidos”.<sup>617</sup> Un sistema democrático implica no sólo elecciones libres, sino también, respecto a la inteligencia, mecanismos de control, transparencia y rendición de cuentas. Desde ese punto de vista, pero también porque la inteligencia estratégica es un asunto de política pública, puede y debe ser discutida por el público, lo cual no significa que la información que maneja sea igualmente pública. Si un gobierno democrático va a tener un servicio de inteligencia efectivo, esos temas deben ser discutidos en público.<sup>618</sup> Estas instancias son las ideales para una reflexión acerca de los ámbitos e instituciones que pueden realizar inteligencia, abriendo la discusión a áreas más allá del ámbito militar y policial.

### Condiciones para que exista inteligencia carcelaria

Se han señalado las razones que desde la teoría y lo deseable, apuntan a incluir el ámbito penitenciario entre los organismos que realizan inteligencia. También se ha visto que, en la práctica, pocos países latinoamericanos dejan abierta -de manera indirecta- la posibilidad de colaboración del ámbito penitenciario (Argentina, Brasil, Chile, Colombia, Ecuador y Guatemala) y si bien se ha visto un avance en la última década respecto de las legislaciones que regulan la actividad de inteligencia, permanecen los desafíos en el ámbito penitenciario para poder incorporarlo a la comunidad de inteligencia. No se presentarán aquí datos que abundan en estudios específicos sobre las cárceles de América Latina,<sup>619</sup> sino más bien se señalarán tres áreas deficitarias que impiden por el momento la integración de la función de inteligencia al ámbito penitenciario y de este mismo a un sistema nacional de inteligencia:

- **Infraestructura carcelaria deficiente:** no sólo la cantidad de espacio es insuficiente para la cantidad de reclusos, sino que también la calidad de la misma. Como consecuencia de ello se presentan altos niveles de sobre- población y hacinamiento, pésimas condiciones sanitarias, altos niveles de violencia y mala distribución de los reclusos de acuerdo a sus características. Con estas condiciones se dificulta la labor de seguridad y el control de la población penal por parte del personal de custodia. Además, son condiciones que facilitan el contagio criminógeno y la comisión de delitos desde la cárcel. Así, cualquier labor de inteligencia se dificulta, y se hace cada vez más necesaria, pues el imperante desorden interno mantiene relaciones tensas, siempre al borde de motines, incendios, huelgas y hechos de violencia. Es un contexto donde muchas veces es preciso para los guardias negociar con los internos para mantener cierto nivel de control. Si esos acuerdos informales no se respetan, se pone en riesgo la seguridad de todos. No obstante, aún en estas condiciones debe existir algún mecanismo para recoger y canalizar información e inteligencia que permitan tomar mejores decisiones para gestionar la actividad penitenciaria y prevenir los hechos mencionados.
- **Débil formación profesional:** para mantener un diálogo entre pares con los organismos de inteligencia del ámbito militar, estratégico y policial, es indispensable mejorar la formación y capacitación del personal peniten- ciario. En muchos casos se forman en sólo pocos meses, en otros so policías que luego de un curso de formación (también breve) pasan al ámbito penitenciario, y en otros ni siquiera existe una escuela de formación. Entregar a los funcionarios una formación profesional, que contemple nociones de seguridad pública, criminología, inteligencia, estrategia, derecho y administración, entre otros, es clave para que ésta área se integre con propiedad al sistema de seguridad, más allá que la naturaleza de su función así lo indique.



- **Controles de seguridad insuficientes:** a los niveles de hacinamiento que dificultan el control, se suma la falta de implementación de tecnologías que apoyen esta labor, como bloqueos de señales de teléfonos móviles y detectores de metales y drogas. Instrumentos que apoyen la labor de seguridad permitirían disminuir los delitos cometidos desde las cárceles, así como mejorar las revisiones a las visitas.

En definitiva, en América Latina en general, existe un acercamiento demasiado centralizado, que no permite iniciar un proceso de experimentación regional o provincial, por ejemplo, respecto al valor para la seguridad pública de su aplicación en el ámbito carcelario. Distinto es el caso del sistema de inteligencia estadounidense, en que, de manera efectiva, los agentes carcelarios no sólo pueden experimentar con la aplicación de métodos de inteligencia al interior de sus cárceles, sino que también tienen la opción de colaborar con los órganos centrales de inteligencia para intercambiar información penitenciaria, por ejemplo, a través de la *Joint Intelligence Sharing Initiative* (Iniciativa Conjunta de Intercambio de Inteligencia) entre el *Federal Bureau of Investigation* (Agencia Federal de Investigación, FBI por su sigla en inglés) y el *Federal Bureau of Prisons* (Agencia Federal de Prisiones, BOP por su sigla en inglés) y del *Regional Information Sharing System Program* (Programa del Sistema Regional de Inteligencia conjunta, RISS por su sigla en inglés) que es lo que hace posible la prevención de la violencia y el resguardo de la seguridad institucional y pública.<sup>620</sup>

Para enfrentar estos desafíos se requiere de una modernización institucional. Esta modernización puede comenzar con la revisión y actualización de las normas, leyes orgánicas y decretos que regulan el funcionamiento, la misión y funciones de las administraciones penitenciarias, que se actualicen dentro de una idea de sistema de seguridad, incorporando la colaboración con otras instituciones. Asimismo, una nueva normativa debería contemplar el desarrollo de escuelas de formación profesionales para los encargados de la administración y la seguridad penitenciaria.

Dentro de estos cambios debiera considerarse también la clara distinción de estructuras encargadas de la seguridad y aquellas encargadas de la reinserción, esto ayudaría a una mejor distribución presupuestaria y de funciones, pues los presupuestos suelen concentrarse en gastos de personal para la seguridad,

## Gestión de Inteligencia en las Américas

con montos inferiores para programas de reinserción social. Una unidad o departamento de inteligencia se ubicaría en el sector dedicado al control y seguridad de los centros penales, en colaboración permanente con las policías y el poder judicial.

De este modo, con estructuras de administración claras, recintos modernos y con adecuado nivel de seguridad, más personal profesional, se podría integrar la administración de los penales a un sistema de seguridad que contempla la inteligencia penitenciaria, como apoyo indispensable especialmente a aquella realizada en el ámbito policial. Se trata de una coordinación que debe explicitarse, pues, como se ha visto, hasta el momento el rol de los sistemas penitenciarios es de eventual apoyo, cuando sean requeridos por estructuras de inteligencia civil, policial o militar, sin continuidad ni permanencia. Pero sin la formación y los recursos profesionales adecuados, este apoyo no dará necesariamente los resultados esperados y el sistema penal no tendrá el lugar que le corresponde en un sistema de seguridad moderno que debe trabajar cooperativamente.

### Conclusiones

Volviendo a las preguntas planteadas en la introducción, se puede señalar primero, que la inteligencia estratégica es deseable en el ámbito carcelario porque se requiere, por vía de intercambios de información e inteligencia, posicionar a las cárceles como un actor activo de la seguridad y la impartición de justicia, dado que desde allí también se organizan delitos de distinto tipo. La labor de inteligencia penitenciaria permitiría mejorar la propia gestión y seguridad de las cárceles y realizar un contacto más eficiente con órganos externos como la policía y el poder judicial.

En términos estratégicos, el valor de la aplicación de inteligencia dentro de instituciones carcelarias, y de compartir información e inteligencia con otros nodos del sistema nacional de seguridad, radicaría en que permitiría una mejor articulación de los medios para conseguir los objetivos de la seguridad. Si se considera en la estrategia de seguridad la trilogía de medios, formas y objetivos en una visión cooperativa, entonces la inteligencia penitenciaria tiene valor en tanto es un medio que también suma información para el objetivo superior de seguridad. Esta visión permitiría salir de una mirada más tradicional de ambos lados: de que las administraciones

carcelarias dejen de considerar que su información es relevante sólo para ellos y de que los otros actores (fuerzas armadas, policías y poder judicial esencialmente) comiencen a verla como una contraparte igualitaria, válida y legítima.

Por último, la gestión eficaz de la función de inteligencia se puede lograr mejorando las inhumanas y poco seguras condiciones carcelarias, pero también estableciendo personal entrenado y dedicado a la producción de información, en lugar de sólo tener guardias y administradores bien preparados. Para ello es necesario que, quienes se encargan de gestionar el sistema penitenciario y el de seguridad y defensa, vean al personal penitenciario de investigación e inteligencia como parte de la comunidad y desarrollen mecanismos comunes de entendimiento y comunicación con el propósito de compartir inteligencia y administrar los riesgos de mejor forma.

De acuerdo a las leyes revisadas, los países de América Latina (Centro y Sudamérica) están lejos aún de llegar a una reflexión sobre sus sistemas de inteligencia que abarque las cárceles. Las nuevas leyes realizadas en la última década con el fin de modernizar la inteligencia no han abordado esta área, conservando visiones tradicionales de la tarea de inteligencia centrada en el mundo militar y policial, aunque dejando abierta -de forma muy vaga- la posibilidad de que otros organismos colaboren, pero en un rol secundario. No obstante, dados los niveles de inseguridad y las manifestaciones complejas de la delincuencia organizada es una reflexión necesaria que debería conllevar a una mejora legal, de gestión y de profesionalización del sector seguridad como conjunto. Este paso hacia adelante debería incluir la inteligencia táctica, es decir, producción de información para el corto plazo para investigaciones, operativos o problemas, e inteligencia estratégica, para apoyar planes de largo plazo, identificar problemas y planificar recursos y políticas en la seguridad carcelaria que tiene también un correlato en el mundo exterior a la cárcel.

### Biografía de la autora

**Liza Zúñiga Collado** Cientista Político, Magíster en Ciencia Política, mención relaciones internacionales por la Pontificia Universidad Católica de Chile. Correo electrónico: llzuniga@uc.cl

## Autonomía del Aparato de Inteligencia, Rendición de Cuentas y Seguridad Interna: Bases para la Supervisión

Russell G. Swenson y Zulia Yanzadig Orozco Reynoso

*¡Ojalá algún poder nos diera el pequeño regalo de vernos  
a nosotros mismos como nos ven los demás!*

—Robert Burns, “A un canalla”, Verso 8

La amistad que se observa entre los funcionarios de inteligencia le da la oportunidad a los servicios de inteligencia de un país de poder ganarse la confianza de otros servicios de inteligencia que operan en el mundo, permitiendo la transmisión de información de inteligencia de manera efectiva e internacional. Sin embargo, este mismo sentimiento entre la comunidad de inteligencia permite que un punto de vista parroquial se introduzca y limite la auto-reflexión necesaria para darle mayor profesionalismo a sus agremiados. Por suerte, algunos observadores astutos, y externos, de prácticas de inteligencia han permitido dar un vistazo al rol social de los servicios de inteligencia que permite el crecimiento profesional entre sus practicantes auto-reflexivos.

Un ejemplo notable de un artículo escrito por alguien ajeno a la comunidad de inteligencia, y con una percepción útil, se publicó recientemente en el *Texas International Law Journal*.<sup>621</sup> El presente ensayo señalará el cómo y por qué este ensayo legal puede considerarse una afirmación de la sabiduría esencial contenida en la famosa frase de Robert Burns. Todos reconocemos que la exposición directa a una cultura extranjera nos permite apreciar la nuestra desde una perspectiva fresca y con renovada apreciación. Así también, es cierto que cuando tenemos la oportunidad de aprender una lengua extranjera comenzamos a entender y apreciar las sutilezas de nuestro propio idioma. Estos hechos aplican al ensayo de Elizabeth Sepper. Para un miembro de la comunidad de inteligencia, versado en las artes liberales y las ciencias, la perspectiva ajena de una disciplina desconocida como el Derecho presenta el reto de entrar en terrenos intelectuales desconocidos. El llegar a entender, en este caso, genera el dividendo de ver a la función de inteligencia de manera holística, tomando en cuenta los intereses de los ciudadanos en un equilibrio significativo de la discreción y la seguridad pública.

En el entendido de que el profesionalismo se genera dentro de la comunidad de inteligencia, debemos comenzar con una definición básica del concepto. Entre los servidores públicos, el profesionalismo significa saber suficiente sobre el ambiente institucional, social y cultural en el que se trabaja de tal manera que se reconozca cuando se promueve el bienestar de la sociedad a la que se sirve, incluyendo, significativamente, si se respetan los principios contenidos en la Declaración Universal de los Derechos Humanos de las Naciones Unidas.

Nuestra autor, Elizabeth Sepper, como es de esperarse, comienza con una revisión bien organizada de la literatura relevante a su tema. Se ve que las redes de transmisión de inteligencia internacionales son extensas y en crecimiento, además de gobernarse a sí mismas, pero con una rendición de cuentas insuficiente por sus acciones ante otros países. Observa que prácticamente todos los servicios de inteligencia en el mundo comparten inteligencia y que este compartir se basa primordialmente en relaciones personales e informales en lugar de tener la autoridad formal de arreglos legales duraderos. Como resultado, existe un déficit tanto en la rendición de cuentas interna como la supervisión externa. En especial le preocupa que la autonomía de la comunidad de inteligencia le da la vuelta a las salvaguardas democráticas prescritas en la ley interna y los tratados internacionales. Además, sugiere cómo hacer que el compartir internacional llevado a cabo por las agencia de internacionales rinda mayores cuentas a los gobiernos y las normas legales internacionales.

El siguiente ensayo surge de la reflexión de los autores sobre la contribución de Sepper y se alimenta de la familiaridad con la creciente literatura del tema, así como por un lado, de más de cuatro décadas de observar y participar en la comunidad de inteligencia de los Estados Unidos (EE.UU.), y por el otro, de observación de la actividad de inteligencia mexicana.

### **El medio ambiente del intercambio de inteligencia internacional**

Varios factores se han combinado para impulsar el desarrollar de relaciones bilaterales y, en ocasiones, redes multilaterales extensas dedicadas a compartir información entre servicios de inteligencia, con relaciones informales aún entre países ideológicamente distintos. Sabemos, por ejemplo, a través de la literatura sobre el tema, que la Agencia Central de Inteligencia de los EUA (CIA por sus siglas en inglés) tiene más de 400 acuerdos de intercambio de

## Gestión de Inteligencia en las Américas

inteligencia con agencias extranjeras (un promedio de más de dos por país) mientras que la Gran Bretaña tiene 120 acuerdos de esta naturaleza.<sup>622</sup> Las necesidades imperantes de la Segunda Guerra Mundial promovieron este fenómeno estando la Oficina de Servicios Estratégicos, precursora de la CIA, a la vanguardia. El ambiente en la comunidad de inteligencia luego de la Guerra Fría introdujo factores aún más decisivos.

La revolución informática que permite la constitución veloz de organizaciones ilícitas, que aumenta su capacidad de acción y que les permite ser altamente móviles, ha creado un medio ambiente que exige una cobertura mundial de pistas para conocer su paradero y actividades.<sup>623</sup> El intercambio de inteligencia ha crecido para cubrir esta exigencia. Otro factor poco notado que genera mayor demanda de intercambio de inteligencia alrededor del mundo es el hecho poco sorprendente de que los servicios nacionales no son eficientes en todas las esferas de inteligencia. La eficacia estadounidense en capacidades de inteligencia técnicas, por ejemplo, es socavada por deficiencias en inteligencia humana (HUMINT).<sup>624</sup> Por tanto, existen fundamentos para que un país intercambie información escasa proveniente de una rama de inteligencia con Estados cuyas habilidades se encuentren en otras áreas.

Donde el intercambio de inteligencia entre dos socios prospectivos no es parte de una red duradera basada en la confianza mutua, existe una estrategia alternativa para generar intercambios útiles. Esta estrategia se conoce como “contrato de relación” un concepto económico que explica cómo socios económicos potenciales pueden cooperar asegurando que ninguna de las partes tenga incentivo suficiente para incumplir el contrato o engañar al socio. Como demuestra el politólogo James Igoe Walsh, una relación jerárquica, donde un Estado más poderoso puede ejercer supervisión sobre las actividades de inteligencia de otro, es exitosa en superar el peligro constante de que la información intercambiada sea deliberadamente incorrecta o inexacta.<sup>625</sup> Como ejemplo se puede citar la relación entre los servicios de inteligencia estadounidenses y colombianos en las operaciones contra el tráfico de drogas y los grupos rebeldes.

Dentro de redes formales y conocidas tales como la OTAN (para la inteligencia militar) y entre las agencias de señales de inteligencias angloparlantes del Reino Unido, EUA, Canadá y Australia/Nueva Zelanda (UKUSA), el intercambio de inteligencia ocurre bajo los auspicios de agencias de gobierno

especializadas en lugar de instituciones de política exterior típicas como el Departamento de Estado de EUA o los Ministerios de Relaciones Exteriores. Además, y esto es lo que más preocupa a Elizabeth Sepper, la decisión de iniciar o terminar con el intercambio es tomada únicamente por funcionarios de inteligencia y por tanto no está sujeta a la supervisión pública o democrática. En la comunidad de inteligencia estadounidense, por lo menos, las acciones de inteligencia encubiertas (negables) deben ser aprobadas por el Presidente y reportadas en tiempo a los comités de inteligencia correspondientes.<sup>626</sup> Sin embargo, no existe dicha provisión con respecto a otras decisiones o acciones de inteligencia.

Si bien es posible que los gobiernos ejerzan presión y control, especialmente sobre sus servicios de inteligencia civiles, usando los contratos de relación como explica Walsh, la esfera internacional básicamente carece de leyes, debido a la ausencia general de la extraterritorialidad de las mismas.<sup>627</sup> En este escenario, los derechos humanos pueden violarse con relativa impunidad, sobretodo por las acciones secretas y negables de organizaciones de inteligencia.

Debido al escrutinio dado a la inteligencia estadounidense, sabemos de un tipo de violación a los derechos humanos que puede ocurrir regularmente. Tal como relata un observador académico de la comunidad de inteligencia, recuerda ocasiones en que funcionarios de inteligencia, en su presencia, recordaban ocasiones en que en países no mencionados la CIA había “reclutado jefes de policía locales para encarcelar a ciudadanos locales con cargos falsos hasta que dichos ciudadanos confesaran a los funcionarios de la CIA lo que querían saber (pero no era de importancia para los jefes de policía locales)”.<sup>628</sup> Este ejemplo encaja dentro del contexto de la colaboración y el intercambio de inteligencia internacional, si bien no es un ejemplo propiamente de un intercambio. Ejemplifica el ambiente sin reglas que impera en las operaciones de inteligencia internacionales.

La preocupación de Sepper es que los servicios de inteligencia pueden dar notoriedad no deseada a sus respectivos Estados, especialmente a través de actos imprudentes. Esta preocupación la lleva a sugerir que el aparato legal tiene una participación esencial como árbitro social de las prácticas de inteligencia.

### El aparato legal como árbitro de la práctica profesional de inteligencia

El material que puede ser estudiado por la comunidad académica legal abarca toda la sociedad y la variedad casi infinita de interacciones entre las personas. Se busca estudiar la creación de reglas que gobiernan dicha interacción y ajustar las leyes a las normas sociales. Sepper ha decidido explorar la frontera del comportamiento extra-nacional de parte de funcionarios públicos cuyos actos como empleados de agencias de inteligencia están fuera del alcance de los sistemas legales nacionales. Si bien los miembros de la comunidad de inteligencia argumentarían que su propia ética profesional es la que guía los límites de su actuar en la esfera internacional, Sepper opina que dicha ética es un sustituto pobre para las leyes que reflejarían de mejor manera los intereses a largo plazo del cuerpo político donde habitan dichos agentes.

La razón principal de la desconfianza de Sepper hacia los servicios de inteligencia es que, sobre todo en relaciones de intercambio internacional de inteligencia, dependen de sus propios procesos de toma de decisiones en lugar de dar cuentas a las normas sociales. Este rasgo independiente de la comunidad de inteligencia lleva a falta de transparencia. Dicha falta de transparencia, a su vez, se deriva de la serie de decisiones a favor de la opacidad que comienza con la protección especial que se da a la información compartida, debido a la insistencia de la agencia fuente de dicha información. Obviamente, si dicha información se vuelve pública, y se rastrea a la fuente, facilitando conocer los métodos de obtención (incluyendo la identidad de informantes), entonces el receptor de dicha información no es de fiar.

El ser de confianza es el *sine qua non* fundamental para los intercambios futuros de información útil. Sepper documenta las razones de su desconfianza mostrando que los servicios de inteligencia pueden aprovecharse de este arreglo de no-divulgación para evadir restricciones legales existentes, en especial aquellas que protegen a los ciudadanos de un país de ser víctimas de intromisión en sus comunicaciones personales, etc. Un ejemplo de mal uso de la confianza de un socio fue cuando los servicios de inteligencia estadounidenses vigilaban a ciudadanos noruegos a pesar de que la policía noruega tenía prohibido hacerlo.<sup>629</sup>



La tendencia de los servicios de inteligencia de volverse menos transparentes conforme se vuelven más autónomos va contra las expectativas o normas democráticas. Inclusive el descubrimiento de actos históricos llevados a cabo por los servicios de inteligencia de un país, a través de procedimientos formales de desclasificación, pueden complicarse si existe información extranjera.<sup>630</sup> De nuevo, dicha información tiene protección especial para generar la confianza necesaria para intercambios futuros. Además, Sepper observa que la vacilación de miembros de la comunidad de inteligencia de revelar fuentes y métodos a través del sistema legal, limita la posibilidad de los medios públicos para supervisar las acciones del gobierno.<sup>631</sup> Cuando hay información extranjera, el incentivo de los servicios de inteligencia de negarse a compartir dicha información con otras agencias nacionales también aumenta la vulnerabilidad de la población con respecto a grupos internacionales cada vez más peligrosos. En el caso de los EUA, la investigación retrospectiva sobre el ambiente de información previo a los ataques del 11 de septiembre revela varias instancias en que dicha información se retuvo demasiado entre las agencias con orientación externa dentro de la comunidad de inteligencia y los ataques tuvieron éxito.<sup>632</sup>

Los académicos legales estudian la aplicación de las normas sociales a la esfera internacional desde la perspectiva del Derecho Internacional, basándose en especial en el cierto éxito que se ha tenido en crear convenciones internacionales, a las cuales pueden adherirse los Estados.<sup>633</sup> Sin embargo, la falta de mecanismos de coerción que acompañen a dichas convenciones significa que no se alcanza el umbral de rendición de cuentas entre agencias gubernamentales.<sup>634</sup> Esta falta de rendición de cuentas obligatoria, salvo en aquellos casos en que dos Estados aceptan jurisdicción internacional para resolver disputas, significa que en el Derecho Internacional, al igual que ocurre en el caso de agencias internacionales que operan en la esfera internacional, la presión entre pares es el recurso principal para indicar lo que es aceptable o no. Sigue sin existir una manera coercitiva de guiar o restringir actos de inteligencia por parte de leyes y acuerdos nacionales o supranacionales.

Por tanto, a pesar de la buena intención por parte de los académicos legales de incorporar a las agencias de inteligencia, y en especial sus actos y acuerdos de intercambio internacionales, a la esfera de aquellos comportamientos sancionados por las normas sociales, la falta persistente de rendición de cuentas que

## Gestión de Inteligencia en las Américas

vemos aplicada al comportamiento estatal con respecto a las convenciones internacionales existentes, insta a buscar un enfoque alternativo para lograr dicha incorporación, al menos en el estado actual de desarrollo o evolución de un diálogo legal que involucre normas internacionales y sanciones efectivas.

La variedad y extensión de comportamientos no-democráticos mostradas en las prácticas de intercambio de inteligencia internacionales, documentadas por Sepper, deben llevar a una exploración seria de estrategias alternativas para lograr la rendición de cuentas democrática así como la supervisión de las prácticas de inteligencia, tanto en la esfera interna como internacional.

### Manteniendo una tradición de autonomía en la toma de decisiones dentro de los servicios de inteligencia

Los jugadores de tenis están familiarizados con el valor dado a que los propios participantes señalen cuando una pelota cae fuera debido a que, aun cuando lo señale el oponente, ambos jugadores reconocen que el jugador más cercano a la pelota tiene la mejor oportunidad de dar el fallo correcto. Es más, cada jugador tiene una buena razón para no hacer trampa – construir una reputación de integridad dentro de un círculo de buenos jugadores. De manera similar, en los servicios de inteligencia nacionales, cuando se debe tomar una decisión crítica sobre la credibilidad de una fuente o la validez de la información, el agente en campo o el analista especializado, y no el asesor de seguridad nacional del Presidente o el comité de supervisión legislativo, debe dar cuentas de lo que puede ser una decisión de inteligencia fundamental. Además, y esto aplica tanto para jugadores de tenis como para miembros de la comunidad de inteligencia, rara vez se toman decisiones individuales sin el escrutinio de al menos unos cuantos espectadores o colegas. Un punto de vista ético con respecto a la rendición de cuentas profesional surge de la conciencia y participación en la legitimización colegial y condicional de nuestras acciones y decisiones. La evolución de esta conciencia ha contribuido a la creación de una nueva revista internacional, en inglés, sobre ética en la comunidad de inteligencia.<sup>635</sup>

El reconocimiento y respeto a la ética profesional apoya continuar con la autonomía sustancial del proceso de toma de decisiones en los servicios de inteligencia para incluir la esfera del intercambio de información internacional señalada por Sepper como ideal para tener una rendición de cuentas más

formal y amplia. Por definición, la función de los servicios de inteligencia es ocupar y actuar en el nicho entre las necesidades de información de los líderes políticos y las fuentes incompletas, y difíciles de obtener, tanto en territorio nacional como extranjero. En este ambiente de información incierto y políticamente denso, la autonomía de la toma de decisiones en inteligencia se vuelve esencial como la base de juicios independientes y objetivos y, de manera colectiva, de la operación independiente de una agencia.

La tradición existente de autonomía en la toma de decisión de los servicios de inteligencia es una costumbre que tiene su origen en la esfera militar. Esto se debe a que en las organizaciones militares relativamente fraccionadas y jerárquicas, la inteligencia está diseñada para, y se espera que tome la iniciativa por delante de la logística, las operaciones e incluso la planeación, sobre todo al tratarse de decisiones estratégicas. Una amistad especial surge entre miembros de la comunidad de inteligencia militar que comparten secretos que no pueden divulgar incluso a sus colegas de operaciones. Esta exclusión aumenta su autonomía y los separa de los “impuros” que no conocen los secretos ni las fuentes y métodos utilizados para obtenerlos. La exclusividad y división derivada de la inteligencia militar, en cuanto contribuye a la sensación de un “club” exclusivo, se extiende a arreglos de enlace extranjeros donde agencias nacionales, por lo general civiles, como la Agencia de Seguridad Nacional de los EUA (NSA por sus siglas en inglés) operan con autonomía profesional extensa.<sup>636</sup>

Al observar el panorama del escenario internacional con miras a examinar la toma de decisiones ética pero autónoma de los servicios de inteligencia, Sepper argumenta que un proceso de culturización, y no la efectividad de posibles sanciones punitivas, explica porque las agencias de inteligencia tienden a alinearse a estándares de comportamiento dictados por las principales agencias de seguridad internacionales. Varios autores, cuya obra ha revisado, explican que la “vergüenza” y el “rechazo” entre miembros de un grupo relativamente pequeño y cohesionados como la comunidad de inteligencia consiguen ejercer presión negativa efectiva. Incentivos positivos incluyen las “muestras públicas de aprobación”.<sup>637</sup> Sepper argumenta que los EUA y el Reino Unido, en particular, han culturizado a sus socios para que adopten estándares de comportamiento relativamente arbitrarios.<sup>638</sup> Es de notar que el Reino Unido es muy sensible a críticas extranjeras hacia la competencia profesional de sus servicios de inteligencia como muestra su intento de evitar

## Gestión de Inteligencia en las Américas

la publicación de *The Spycatcher*, que expone las acciones ilegales e incompetentes dentro del servicio de inteligencia interno civil, el MI5, cuyo autor fue el director general adjunto de dicha agencia.<sup>639</sup>

Estados con poder político como los EUA, a través de los actos y reputación de sus agencias de inteligencia, pueden culturizar (con o sin incentivos financieros y de entrenamiento) a socios existentes y potenciales para que usen el polígrafo para contratar empleados, aceptar el término “anti-terrorismo” para agrupar actividad criminal y políticamente orientada y finalmente, para desarrollar y emplear agencias de seguridad nacional (de inteligencia militar así como agencias civiles con orientación internacional) en lugar de instituciones policíacas nacionales o incluso internacionales.<sup>640</sup> Por tanto no es el “control” externo ejercido por poderes judiciales, legislativos o ejecutivos que hace que la toma de decisiones en materia de inteligencia cumpla con la norma internacional, sino más bien es el proceso social de culturización a estándares profesados por Estados líderes y poderosos.

Debe reconocerse una reserva con respecto a la rendición de cuentas interna de los servicios de inteligencia. Dicha reserva es que la rendición de cuentas entre los servicios de inteligencia de seguridad nacional existe como una serie de decisiones inmediatas y no como una preocupación a largo plazo o consistente. El lograr mayor consistencia requiere de mayor atención a tendencias de largo plazo esbozadas por ideas e ideales políticos con alcance global. Otra razón por la cual estos servicios carecen de representación establecida por parte del cuerpo político entero de sus países es que las agencias civiles en particular son instituciones relativamente nuevas, que datan cuando mucho desde la Segunda Guerra Mundial y, en su forma actual, desde el fin de la Guerra Fría. De manera importante, la sensación de inmediatez que permea la rendición de cuentas en los servicios de inteligencia deriva de una enfoque necesario en el actuar futuro en lugar del transcurso de la historia, lo que los vuelve más o menos aislados de la base de ética y rendición de cuentas de la sociedad en general donde las leyes que representan el *zeitgeist* evolutivo de la sociedad se han desarrollado y aplicado con base en la voluntad popular y el proceso político. Por tanto, debido a la preocupación de que las instituciones y personal de los servicios de inteligencia de seguridad nacional rindan cuentas de manera general y sean sujetos a supervisión legal, debemos buscar un modelo funcional y universal de institución de seguridad nacional que puede ostentar legítimamente

los beneficios de la autonomía de la toma de decisiones en el proceso de recolección de información de inteligencia, y al mismo tiempo representar las normas de comportamiento y actitud de su sociedad en general.

### El modelo de inteligencia policial para la supervisión y rendición de cuentas profesional

La sustitución del concepto de “seguridad pública” en lugar de “seguridad nacional”, la mayor popularidad de la actividad policíaca comunitaria y el surgimiento de la actividad policíaca basada en inteligencia en varias partes del mundo señalan mayor integración del interés local con el nacional en cuanto a la seguridad personal y la responsabilidad cívica.<sup>641</sup> Michael Herman, observador prominente de asuntos de inteligencia internacionales afirma que “Si bien un solo Estado (o coalición de Estados) puede ganar una guerra, un tratado de comercio o una disputa fronteriza, la mayoría de los Estados se benefician de menor narcotráfico o terrorismo – no es un juego suma cero”.<sup>642</sup> ¿Puede aplicarse lo mismo a lo que ocurre en un país? Para que lo anterior sea cierto en un solo país en particular, debe haber una aplicación equitativa de medidas para mejorar la seguridad pública a lo largo de todo su territorio. Dada la movilidad de organizaciones criminales sofisticadas, si esta mejora geográficamente equitativa no ocurre, entonces la eliminación de la actividad criminal que atenta contra la seguridad pública puede llevar a que dicha actividad surja en aquellos lugares donde no es combatida con vehemencia. Como bien saben aquellos familiarizados con el género “*Western*”, el aplicar la “ley y el orden” en las regiones remotas dependía de la demanda local por un alguacil confiable, respaldado por agentes federales despachados regionalmente. Este hecho hace que la policía comunitaria y guiada por inteligencia sea el nuevo elemento esencial en la frontera de información donde las tensiones entre la actividad criminal y la seguridad pública exigen solución. También es de esperarse que las organizaciones criminales hayan descubierto la sinergia entre la planeación con base en inteligencia y el reclutamiento local en sus propias operaciones.

Sepper argumenta que si los miembros de la comunidad de inteligencia permitieran que sus prácticas fueran revisadas por el sistema judicial en sus respectivos países, entonces “el arresto y enjuiciamiento de los sospechosos, y no su detención y tortura...detendría los abusos y generaría apoyo popular”.

## Gestión de Inteligencia en las Américas

Recomienda además que “se debe considerar al terrorismo como un acto criminal – que debe ser tratado a través de los sistemas legales de acuerdo con la ley, la democracia y los derechos humanos”.<sup>643</sup> Con la etiqueta del terrorismo, el sistema de inteligencia de los EUA se ha culturizado a sí mismo y a sus socios para que mantengan actos anti-terroristas internos e internacionales con motivos ideológicos fuera del sistema legal de la policía, los abogados y jueces.<sup>644</sup> De manera coloquial, los funcionarios de inteligencia temen que fuentes y métodos sean expuestos en las cortes. Sepper, sin embargo, argumenta que “las cortes son adeptas en encontrar soluciones creativas para proteger información y permitir una defensa eficaz”.<sup>645</sup> Agrega que “la participación de las cortes tiene varias ventajas claras. Promueve el interés de la inteligencia occidental por la precisión y búsqueda de la verdad, que facilita la protección de los Estados democráticos, objetivo fundamental de la misión de dichas agencias”.<sup>646</sup>

Un resultado de la tendencia de mantener la inteligencia de seguridad nacional al margen de los sistemas policiales y legales es que las agencias policíacas han tenido que desarrollar redes internacionales e informales que dependen de la buena voluntad individual y la habilidad de los funcionarios gubernamentales para compartir información sensible sin contar con la aprobación formal de funcionarios de alto rango.<sup>647</sup> Debido a su naturaleza informal y no-oficial, este enfoque puede derivar en la falta de fondos continua de la actividad policíaca comparada con lo que se destina a instituciones de seguridad nacional/inteligencia que se arropan y actúan bajo la bandera del “anti-terrorismo”.

Por supuesto que el enfoque “anti-terrorista” contra el comportamiento ilícito gana apoyo popular cuando figuras claves y odiadas son capturados o asesinados. Sin embargo, el enfoque de justicia criminal recomendado por Sepper, que consiste en usar mayormente agencias policíacas, guiadas por sus capacidades de recolección de inteligencia, contra cualquier objetivo, con o sin motivación ideológica, a fin de lograr ambos aspectos clave de la rendición de cuentas (transparencia y ser sujeto a sanciones negativas o positivas), continua recibiendo relativamente pocos fondos.<sup>648</sup> Donde esto ocurre, hay una desconexión (y no simple tensión) entre la falta de recursos destinados para cumplir con la exigencia social de seguridad pública a través del marco legislativo y legal, y la abundancia de recursos disponibles para los servicios de inteligencia nacional, que no rinden cuentas.



Figura 9. Equipo de marina mexicana

Fuente: Foto por Zulia Orozco

Como ejercicio para reducir esta desconexión, una nueva ley fascinante en el estado mexicano de Nuevo León es una iniciativa sub-nacional poco común que debe ayudar el esfuerzo de la justicia contra grupos narcotraficantes que utilizan “halcones” para espiar a la policía.<sup>649</sup> En dicha ley, de acuerdo con dos investigadores de inteligencia estratégica del Tecnológico de Monterrey, se establecen, por primera vez, sanciones criminales para aquellos que sirven de halcones durante operaciones de narcotraficantes en el estado. Este recurso legal respaldará cualquier esfuerzo de los operativos policiales para identificar e interrogar al menos a los que participan en esta forma de colaboración local con los grupos criminales. La posibilidad de ir a la cárcel puede incentivar a los halcones capturados a proporcionar mayor información sobre la actividad criminal. Por el momento, esta iniciativa se ha limitado a un estado de México pero, si se emplea de manera exitosa, puede indicar un cambio en la tendencia de asignar recursos nuevos en mayor medida a las fuerzas de seguridad pública nacionales.

Podría preguntarse si las agencias policíacas, cuando realizan operaciones de inteligencia, cumplen con preceptos internos de rendición de cuentas en su

## Gestión de Inteligencia en las Américas

toma de decisiones. Debido a que las instituciones policíacas están enraizadas en el sistema legal de un país, y dado que su recolección de evidencia pasa por un proceso abierto y oral en la corte, dicho proceso otorga la transparencia que es un aspecto importante de la rendición de cuentas. ¿Existen además sanciones contra el obviar procesos legales formales (debido proceso)? En esta instancia, como una medida de rendición de cuentas que busca asegurar que los derechos humanos no sean violados por funcionarios de la ley en la recolección y uso de información de inteligencia, se observa que la afinidad cultural del uso del polígrafo entre agencias de inteligencia militar y civil estadounidenses para actividades de contra-inteligencia se ha extendido a socios en la materia. En México, por ejemplo, el polígrafo se ha usado como una “prueba de confianza” aplicada incluso a empleados veteranos.<sup>650</sup> Con la confianza de que tanto la transparencia y las sanciones negativas están presente, se cubren ambos aspectos de la rendición de cuentas.

Las agencias policíacas comunitarias, paramilitares, cuando emplean violencia desproporcionada, son acusadas de adoptar un estilo militar demasiado agresivo. La militarización de las agencias policíacas tiene una contraparte potencial al nivel nacional e internacional: la policialización del ejército. La policialización puede concebirse como la tendencia del ejército a usar en menor medida la fuerza descubierta. Un ejemplo de este enfoque desde la



Figura 10. Miembros de la unidad especial operativo de policía "Zorros"

Fuente: Foto por Zulia Orozco



perspectiva de la inteligencia es las operaciones de inteligencia militares de los Estados Unidos en Iraq y otros países.<sup>651</sup> Como describe un participante, los operativos del Comando Conjunto de Operaciones Especiales han comenzado a utilizar en menor medida los métodos de interrogación coercitiva para obtener información de detenidos comunes quienes son liberados si su información resulta ser útil y veraz.

Si un propósito central del personal militar interno es usar sus capacidades de inteligencia para encontrar informantes y desarrollar relaciones comunitarias, entonces se vuelve posible que el ejército utilice métodos menos coercitivos. Un ejército guiado por actividades de inteligencia para afilar las herramientas de las fuerzas de seguridad nacional, no debe ser sorprendente dado que la inteligencia tradicionalmente ha sido reconocida como el elemento guía dentro de las funciones militares especializadas. ¿Se observa en este escenario un modelo para la integración de la policía local con capacidades de inteligencia nacional apoyadas por instituciones militares o civiles nacionales?<sup>652</sup>

La Policía Federal Preventiva<sup>653</sup> mexicana es la institución más avanzada del país, en términos de su función de inteligencia preventiva. Cuenta con todos los recursos necesarios para sus propias investigaciones. La labor de investigación de los autores revela que la policía estatal más avanzada de México (aquella del estado de Querétaro) cuenta con bases de datos que le permite generar inteligencia preventiva. Esta herramienta permite a las organizaciones policíacas comparar información criminal y tomar acciones proactivas; sin embargo, la mayoría de las instituciones estatales responsables de la seguridad pública (como ocurre en los estados de Yucatán o Zacatecas) carecen de personal calificado y, además, los agentes temen ejercer al máximo su rol institucional, ya que el Estado mexicano no puede asegurar su seguridad personal contra el crimen organizado.<sup>654</sup>

Hechos recientes en México ofrecen un estudio de caso de como la recolección de información por parte de la policía local ha sido usurpada por fuerzas militares. En diversas localidades de México, las fuerzas militares han desplazado a las policías locales.

Una entrevista de uno de los autores a un funcionario de policía local que trabajaba en un municipio donde el ejército ha tomado control de la seguridad, revela algunas de las dinámicas que acompañan la pelea entre las instituciones

## Gestión de Inteligencia en las Américas

locales y las de seguridad nacional e inteligencia. El funcionario expresó que a pesar de que cuentan con el equipo técnico necesario para alertar al Gobierno Mexicano sobre la presencia de actividad criminal, a través de la *Plataforma México* (la base de datos principal sobre el crimen organizado), las autoridades administrativas del municipio prohibieron agregar comentarios o subir información a la plataforma sobre situaciones serias como tiroteos o secuestros. La razón tras esta orden era claro: el temor.

De acuerdo con la persona entrevistada, las autoridades policíacas administrativas temían que se dieran dos escenarios, el primero de los cuales es ya realidad:

1. Temor de que el Gobierno Federal enviara más tropas al área, y
2. Temor de que el Gobierno Federal no destinara recursos financieros para programas de seguridad pública como el Fondo de Asistencia de Seguridad Pública (FASP) y los Subsidios para la Seguridad Pública en los Municipios (Subsemun).

Sin embargo, luego de una reflexión personal sobre las consecuencias potenciales y las sanciones administrativas que podrían resultar de estas acciones negligentes, el personal administrativo cambió de parecer y decidieron permitir el subir información sobre cualquier situación a la base de datos. De cualquier manera, el entrevistado confirmó que, dada la situación tan violenta, el personal militar asumió el control completo de las instalaciones policíacas locales en 2011. De acuerdo con un agente, los policías fueron cesados sin discusión alguna y luego estaban a disposición de un programa de certificación, y el ejército permanece a cargo de la seguridad del pueblo.

Desde una perspectiva ciudadana, en años recientes, el fenómeno de la seguridad pública se ha visto como un problema cada vez mayor. Sin embargo, esto es cuestión de percepción, ya que los datos son variables. De acuerdo con el Instituto Ciudadano para el Estudio de la Inseguridad, la confianza pública en la Policía, comparada con la que se tiene en el Ejército, es relativamente baja.<sup>655</sup> Los datos de encuestas revelan desconfianza e incluso una relación fragmentada entre la policía y la comunidad, debido evidentemente a la opacidad, corrupción, ineficiencia e ineffectividad de la labor policíaca que incluye, entre otras cosas, la tarea peligrosa de inteligencia policíaca.



Figura 11. Equipo policía federal mexicano

Fuente: Foto por Zulia Orozco

Una condición para el éxito de la inteligencia policiaca, como parte DE una agencia de seguridad auténtica y de servicio a la comunidad, suponiendo que obtengan paridad presupuestal con las instituciones de seguridad nacional, será la evolución de la sociedad hacia cortes independientes y acusatorias así como procesos judiciales exitosos. La mejor información de inteligencia proviene de participantes que informan a las autoridades gubernamentales sobre actos criminales futuros; por tanto, los programas de protección de testigos son necesarios para familias completas para mostrarle a informantes potenciales que provee información no es una sentencia de muerte. En sociedades

donde las familias completas pueden ser víctimas, es esencial para el proceso judicial que existan informantes gubernamentales encubiertos cuya identidad pueda ser protegida. En ausencia de elementos de inteligencia humana que puedan entrar en los círculos íntimos de criminales locales,<sup>656</sup> la mejor alternativa es de naturaleza “técnica” – la capacidad probada de la interceptación de comunicaciones que proporcionan evidencia criminal relativamente sólida. El producto de la inteligencia técnica no revela la identidad del recolector, aun cuando algunos detalles para la recolección efectiva fuesen proporcionados por informantes “internos”. Dichos individuos pueden permanecer en el anonimato en la corte. Un escenario probable sería que el informante surgiera de la localidad afectada y que la tecnología para recolectar y procesar las comunicaciones fuese un recurso estatal o nacional. En este escenario, la ética comunitaria y los recursos provenientes de un gobierno representativo se unen para obtener las preferencias individuales y colectivas de la ciudadanía, trayendo a fruición por tanto el ideal ético de atar la actividad de inteligencia a los valores de la sociedad.

### Descubrir el modelo preferido para la supervisión y rendición de cuentas democrática en materia de inteligencia

Tal como señala la académica legal Elizabeth Sepper, la autonomía desmedida de las prácticas de intercambio de inteligencia internacionales debe abordarse para proteger los ideales democráticos. La revisión de su trabajo por parte de los autores, desde una perspectiva de inteligencia gubernamental, va de un examen de validez de su argumento de que el sistema legal de una democracia puede lograr correctamente una reducción en la autonomía de los servicios de inteligencia, a una evaluación de los enfoques alternativos que pueden lograr un nivel adecuado de rendición de cuentas y supervisión en materia de inteligencia. La supervisión existe dentro de un marco legal diseñado e implementado por los poderes legislativo y judicial en una democracia eficaz. La rendición de cuentas implica apertura por parte de las agencias de inteligencia profesionales a que sus prácticas sean inspeccionadas así como la aplicación de sanciones negativas y positivas, incluyendo especialmente la aplicación de prioridades presupuestales, a su trabajo.

Resulta que el deseo por parte de los académicos legales de lograr una función arbitral con respecto a la conducción de la actividad de inteligencia, al menos a nivel internacional, aún no logra la rendición de cuentas deseada. Esto se

debe principalmente a que no existe un mecanismo confiable para sancionar dicha actividad. Las agencias policíacas guiadas por actividades de inteligencia pueden lograr la rendición de cuentas auténtica y, debido a que son parte integral del sistema judicial, están orientadas de origen hacia el rigor de la supervisión legal.

Una versión distinta de este artículo apareció en el sitio electrónico del Instituto de Seguridad y Democracia (Insyde), un centro de estudios en seguridad, en <http://www.insyde.org.mx/shownews.asp?newsid=708>.

### **Biografías de los autores**

**Russell G. Swenson** trabajó desde 1988 como profesor, y desde 1995 hasta 2008 como Director de Investigación Aplicada en el Colegio de Inteligencia de Defensa Nacional (NDIC por sus siglas en inglés), ahora la Universidad Nacional de Inteligencia. También ha sido director de la NI Press desde su creación en 2006. Es autor y editor de numerosas publicaciones sobre el proceso de inteligencia (<http://www.niu.edu/ni-press/press.html>). Anteriormente, trabajó como analista de inteligencia y lingüista en la Fuerza Aérea estadounidense y como profesor de Geografía en la Universidad Occidental de Illinois. Cuenta con estudios de licenciatura de la Universidad de Kansas (Geografía, Español, Estudios Latinoamericanos) así como de posgrado de la Universidad de Wisconsin-Milwaukee (Maestría y Doctorado en Geografía). Ha sido galardonado con la Medalla de Mérito en inteligencia nacional. Ya jubilado, continúa colaborando con funcionarios e investigadores en el área de inteligencia estratégica. Correo electrónico: [drintel2@yahoo.com](mailto:drintel2@yahoo.com).

**Zulia Yanzadig Orozco Reynoso** cuenta con Maestría en Derecho y Licenciatura en Sociología por la Universidad Nacional Autónoma de México. Colaboró como investigadora de diversos proyectos en el Instituto de Seguridad y Democracia. Fue coordinadora institucional para el Informe de Seguridad Ciudadana en América Latina, 2013. Es el primer informe regional del sistema de Naciones Unidas, especializado en temas de seguridad ciudadana y desarrollo humano en 19 países latinoamericanos. Sirvió de titular del área de investigación de Rectoría, de la Universidad Nacional Autónoma de México (UNAM). Se especializa en temas de violencia y seguridad y está doctoranda en la Universidad Nacional Autónoma de México. Correo electrónico: [zulia.ozco.pnud@gmail.com](mailto:zulia.ozco.pnud@gmail.com).

## Sección IV

# Gestión de Integración— un Reto para los Servicios de Inteligencia



### Educación e Integración en Inteligencia: Una Relación Simbiótica

Anne Daugherty Miles

Como es mencionado en la tercera sección del libro, puede existir una “pared”, real o percibida, que inhibe el intercambio de información y prospectiva entre el mundo de la inteligencia policial y la de seguridad nacional. Adicionalmente, la separación funcional y geográfica puede crear o acrecentar las diferencias de cultura organizacional o de tecnología que impiden los deseos de colaboración. A veces estos obstáculos pueden ser superados por una iniciativa legislativa. En la década de los 80, por ejemplo, el Congreso de EE.UU. dirigió la necesidad prioritaria de integrar culturas específicas del servicio operativo de las Fuerzas Armadas, aprobando una ley conocida como “*Goldwater Nichols Act*”,<sup>657</sup> la cual ordenó y premió la adopción de una “acción conjunta”, y a la vez obligó a una “educación militar profesional conjunta”. La relación de la educación con la deseada “acción conjunta” se concretó, y se dedicaron los recursos para la transformación del entonces existente sistema de educación militar con énfasis en la integración.

José Paz, en su contribución, “La Formación del Profesional de la Inteligencia Estratégica: Realizando Expectativas Nacionales”, sugiere que una orientación más conjunta o holística a la educación en inteligencia será el principal derrotero para lograr un nivel de integración funcional y de pensamiento innovador para hacer frente a problemas urgentes, como la ciberseguridad. Paz argumenta que la educación en inteligencia crea “conocimientos profundos”, y que sus huellas perdurarán durante toda la trayectoria profesional. Adicionalmente, cree que la libertad académica es menester, junto con el espacio psicológico, para la creatividad, una ampliada interacción personal, y fuerte investigación. Seguidamente, Paz cree que la educación es el vehículo para enseñarnos a pensar de modo crítico, cuestionar suposiciones, y afinar las destrezas de analizar cuidadosamente y de pensar en términos abstractos.

Cada vez más, los problemas que amenazan la seguridad ciudadana y nacional de nuestros respectivos países necesitan de actores diversos para sustentar una colaboración en beneficio de un análisis de largo plazo que sea a la vez holístico, bien pensado, y estratégico. Parece no haber otro lugar mejor que una escuela de posgrado para afinar las destrezas y desarrollar una red de



contactos y amigos duraderos. Eso queda claro especialmente si se asocian actores no sólo de los sectores de la defensa, de la inteligencia y de la aplicación de la ley, sino también de las comunidades académicas y del ámbito de los negocios. Efectivamente, en su ensayo, Paz argumenta que estas instituciones de educación ocupan el espacio perfecto para mediar los universos paralelos de los sectores público y privado. Mientras muchas de las instituciones de educación en inteligencia optan por mantener sus aulas cerradas a los que no se identifican como miembros de los servicios de inteligencia, Paz recomienda lo contrario – que las escuelas se abran a todos los interesados: “el secreto es propio para los temas en los que la ley lo prescribe, pero éste no puede extenderse al mundo académico”. Este autor prefiere relegar el régimen del secreto para los cursos de entrenamiento, y una apertura a sedes educativas para dar una luz a los grandes problemas de la actualidad – aquellos problemas que requieran para su solución la sabiduría colectiva de las mejores mentes de la nación. “[N]o es necesario ni conveniente incursionar en cuestiones secretas para que lo académico tenga éxito, más aún cuando en la actualidad gran parte de las actividades de inteligencia se desarrollan a partir de fuentes abiertas”.<sup>658</sup>

Como es sugerido en el ensayo introductorio del libro, hemos llegado a depender de una inteligencia oportuna y precisa para la “seguridad pública, la planeación civil y militar, e incluso hasta para nuestro bienestar económico.” Son tan acentuadas las manifiestas amenazas, que surge la necesidad de una integración de todas las fuentes de inteligencia -sean del sector público o privado- como una demanda inmediata e imperativa.

Esta es, de hecho, la idea central del ensayo de Robin Rogers sobre la seguridad del ciberespacio, el segundo trabajo de esta sección. En su ensayo, Rogers encierra admirablemente la necesidad de una integración de todos los niveles del gobierno para compartir la información que tenga que ver con las pretensiones de intrusiones y de ataques desde el ciberespacio en todas las esferas de lo público y lo privado. Nos hace recordar que estas pretensiones ocurren diariamente, y que la integración es necesaria, o parafraseando sus palabras, el ingrediente esencial de esta coordinación es compartir información, ya sea información patentada, información para la aplicación de la ley o información de inteligencia.

Rogers destaca la falta de un esfuerzo integrado de todos los recursos gubernamentales, y de sus niveles varios, para enfrentar la amenaza que surge en el

## Gestión de Inteligencia en las Américas

terreno de la seguridad cibernética. El crimen cibernético es de índole “interméstico”,<sup>659</sup> en el sentido que se ve en ello igualmente un desafío doméstico e internacional, y por eso se supone una amplia gama de actores involucrados en el área de seguridad gubernamental. Los otros dos ensayos plantean una resolución práctica para la superación de los obstáculos al intercambio e integración de información entre países, problema mencionado también por Rogers. El ensayo de Paz presenta una solución educacional; Brei et al. recomiendan la construcción de un equipo de trabajo innovador. Ambos se orientan al logro de interacción colaborativa, junto con el pensamiento integrado.

El ensayo de Rogers toma en cuenta los ensayos de las primeras tres secciones del libro que destacan varios obstáculos a la colaboración esperada para el intercambio de información. Nos recuerda que las barreras incluyen las dudas sobre qué se debe compartir, “territorialismo” institucional, cuestiones de confianza, y problemas respecto al abuso potencial de libertades civiles y derechos humanos. Incluidos como obstáculos al intercambio de información son los que resultan de una separación institucional – tanto geográfico como funcional. Rogers agrega a su ensayo que “Estos obstáculos se ven agravados cuando los países necesitan intercambiar información de inteligencia entre sí.”

El ensayo de Brei, Frensley y Roberts, (los tres veteranos de la Fuerza de Asistencia de Seguridad Internacional—ISAF—de Afganistán) evidencia cómo una misión dedicada a asesorar y promover el desarrollo de instituciones gubernamentales a nivel nacional, requiere de una filosofía innovadora en la creación y manejo de información para lograr una gestión adecuada de interrelaciones personales y profesionales con homólogos de la nación anfitriona.

Se explica cómo la formación de un equipo pudo superar los límites legales y organizacionales que normalmente son asociados con operaciones formales de inteligencia. Su habilidad para transformar la perspectiva del cuerpo asesor del “conocimiento situacional” dependía de la combinación profunda y amplia de la información social política tanto de los EE.UU. y de los ministerios del gobierno. Los autores están de acuerdo con el deseo de una alianza para abrirse a todo, y escriben sobre las formas empleadas para mantener las relaciones basadas en la confianza con sus homólogos. Creen que el equipo de su creación “captura las perspectivas generadas por sus diferentes componentes a nivel operativo y las transforma en conocimientos compartidos por toda la organización.”

Los autores plantean que “toda misión de asesoramiento del sector seguridad es iniciativa de ‘*smart power*’”. Con esto quieren decir que su misión era una contribución por parte de *soft power* a la estrategia *smart power*, la cual incorporaba elementos de *hard power* (asociado con fuerza militar o el “garrote” económico), y *soft power* (asociado con diplomáticos o la ayuda humanitaria o la “zanahoria”). El invertir recursos en alianzas o mediante otro tipo de colaboración es ingrediente imprescindible del *soft power*, según su definición por Joseph Nye y otros. Se puede decir que este ensayo así indica que la adopción de un equipo de esta índole es asociada con el éxito de este tipo de misión, y en consecuencia, se hace válida la estrategia.

En su totalidad, estos tres ensayos revelan unas verdades sobre el valor de la educación y la integración en inteligencia. En el primer plano, Rogers considera a ambas como ingredientes imperativos para resolver grandes problemas que tocan la seguridad del ciberespacio. El argentino Paz considera que la integración refuerza la innovación cuando existen instituciones de educación en el tema de carácter amplio, sirviendo a todo un sistema o comunidad de inteligencia. Finalmente, Brei et al. describen un proceso de integración en el que el acto mismo de integración de inteligencia educa no sólo a esos quienes la reciben, sino también a todos aquellos que la hacen. De hecho, Brei et al. sostiene que una meta principal de la integración en inteligencia debe ser la creación de “capital intelectual”, es decir, conocimientos que existen como producto de “la materia intelectual cruda generada por los funcionarios.”

Tte. Cnel. **Anne Daugherty Miles** (en retiro de la USAF) cuenta con un doctorado en Políticas Americanas de Georgetown University. Desde 1995, ha sido parte del cuerpo docente de la Universidad Nacional de Inteligencia. Sus especialidades son el manejo de recursos y el proceso de formulación de políticas, ambos temas orientados al ámbito estadounidense doméstico, tanto como al contexto de políticas internacionales. En 2009, la Dra. Miles sirvió como socio del grupo asesor para la Comisión de Fuerzas Armadas en la Cámara de Diputados, y en 2010, como Asistente Legislativa para un Diputado de esa institución. Su apremiado ensayo sobre “La Educación Profesional en Inteligencia” se puede encontrar en la página de la *International Association for Intelligence Education* <http://www.iafie.org/>. Correo: [amiles@crs.loc.gov](mailto:amiles@crs.loc.gov).

## La Formación del Profesional de la Inteligencia Estratégica: Realizando Expectativas Nacionales

José Gabriel Paz

*Dimidium facti, qui coepit, habet; sapere aude, incipe.*  
(*Quien ha comenzado, está a medias: atrévete a saber, empieza!*)

—Horacio, “Epistularum liber primus” Epístola II

### Introducción

Sin duda alguna, la actividad humana de mayor relevancia, es la transmisión de conocimiento, y esto es así por cuanto la cantidad de información que la especie humana transmite genéticamente es insuficiente para el desempeño social de un individuo,<sup>660</sup> es por ello, que la educación es un proceso indispensable para la existencia y subsistencia del hombre.

La educación es una actividad permanente que se inicia en el ámbito familiar y en su contexto social, y es continua porque se da a lo largo de toda vida. Se inicia en la edad pre-escolar y alcanza los postgrados, re-entrenamientos, calificaciones y autoeducación, lo que permite al ser humano mediante la capacitación constante, mejorar su calidad de vida y su desempeño laboral.<sup>661</sup>

Esa tarea de capacitación constante que cumple la educación, adquiere una gran importancia cuando se trata de formar a los individuos en niveles superiores del conocimiento, donde es necesario alcanzar calidades y cualidades sustantivas que les permitirán desarrollarse para cumplir funciones en la sociedad y en las instituciones. Sin embargo, la tarea educativa toma dimensión superlativa, cuando se trata de formar al personal de ciertas organizaciones del Estado, como son las estructuras de inteligencia estratégica, en las que se cumplen complejas y específicas labores.

Así, el presente trabajo busca determinar algunos criterios a tener en cuenta en una formación profesional de excelencia, y cómo se podría evaluar el mérito de la educación en términos prácticos.

## Responsabilidad institucional y educativa en la profesionalización del personal de inteligencia

La profesionalización es el pilar de una organización de inteligencia estratégica sólida, estable, con objetivos claros y con una cultura institucional sustentada en principios y valores. Para ello deben contar con una burocracia estable, especializada, originada en un sistema de reclutamiento y de selección apropiado basado en rigurosos criterios, que promueva la educación superior como condición de ingreso, que cumpla con procesos de formación y capacitación que garanticen la calidad técnica de su material humano, y que a su vez conforme una carrera que brinde posibilidades de ascensos en función a criterios de aptitud y bajo los principios de objetividad, igualdad de oportunidades, mérito y capacidad.

Ciertamente la profesionalización ya ha dejado de ser un proceso empírico o pragmático, puesto que el conocimiento se convierte cada vez más en una exigencia necesaria para la calificación que las actuales circunstancias requieren. Así, las capacidades profesionales de quienes trabajan en el ámbito de la inteligencia, van desde el nivel técnico hasta el nivel de postgrado universitario, donde en todos los casos se requiere el conocimiento profundo de las diversas ramas de su ámbito de investigación.

Pero es misión ineludible de la organización de inteligencia la búsqueda de la calidad institucional y la excelencia en su personal. Por ello deberá contar con profesionales formados en centros educativos de alto nivel académico, que además de dotarlos de las capacidades y destrezas, y de desarrollar o amplificar las habilidades y aptitudes nativas específicas y necesarias para su función, generen en el individuo valores y hábitos que generen el respeto a la ley y a los derechos humanos, que cimienten en ellos una conciencia ética, solidaria, reflexiva y crítica, así como también, promuevan la lealtad y el amor a su país y a su profesión.

Debe ser una meta institucional en la organización de inteligencia de cada país, el velar permanentemente por mantener a su personal dentro de elevados estándares de calidad académica. También deberían ser metas, que la enseñanza se enmarque en el sistema educativo del país al que pertenezca, que se cumpla dentro de instituciones de educación superior, (sea con recursos educativos propios de la organización o a través de otras instituciones

## Gestión de Inteligencia en las Américas

educativas), que sea posible que los estudios se lleven a cabo dentro del nivel de postgrado, y que se desarrollen procesos de reentrenamiento o recertificación basado en un programa de educación continuada.

Para brindar la educación del nivel que se pretende, se requiere de apertura académica, creatividad, interacción y dinamismo, aunque pareciera que estos criterios se contraponen con el secreto del ámbito profesional. Sin embargo, debe tenerse en cuenta que el secreto es propio para los temas en los que la ley lo prescribe, pero no para lo académico, no es necesario ni conveniente incursionar en cuestiones secretas para que lo académico tenga éxito, más aún cuando en la actualidad gran parte de las actividades de inteligencia se desarrollan a partir de fuentes abiertas a las que puede acceder cualquier ciudadano común, y sólo una ínfima parte de esta actividad tiene que ver con informaciones obtenidas a través de medios excepcionales.<sup>662</sup>

El concepto de amplitud académica debe primar tanto para el tratamiento libre de los temas en el marco educativo, como para la participación de amplios sectores de interés en esta temática.<sup>663</sup>

La amplitud educativa, es necesaria por cuanto

los centros de formación pública de inteligencia no pueden hoy restringirse únicamente a la preparación de su propia burocracia de analistas de inteligencia y agentes o gestores de contrainteligencia, sino que deben ampliar su radio de acción y preparar a otros funcionarios públicos diferentes en el conocimiento y cultura de inteligencia, como los parlamentarios miembros de las comisiones especializadas de inteligencia y, especialmente, de sus asesores legales y técnicos, que en muchos casos, sus criterios y formación de derecho público, constitucional y procedimiento parlamentario en la elaboración de leyes de inteligencia o en la realización de tareas de fiscalización, debe ser complementado con conocimientos en asuntos de seguridad nacional e inteligencia. El mismo camino debe tomarse en el caso de jueces y magistrados del Poder Judicial encargados de autorizar las operaciones especiales de inteligencia y de sus funcionarios adjuntos y auxiliares de administración de justicia.<sup>664</sup>

## El valor y necesidades educativas del personal de inteligencia

Los analistas de información, los servicios de estudio, análisis y prospectiva, y los equipos de planificación estratégica, confluyen en la tarea de producción de inteligencia estratégica.

En general los analistas conforman el personal especializado que desarrolla la tarea de análisis dentro del organismo de inteligencia, realizan el estudio valorativo de la información sin refinar del que se deducirán los elementos válidos o útiles para el consumo específicos de inteligencia. O sea, deberán realizar una tarea deductiva de los elementos, en la que se extraen productos significativos como la valoración de la fuente, la interpretación de procesos y de su contexto, así como establecer su significación como instrumento de inteligencia. Junto a los analistas están los servicios de estudio, análisis y prospectiva, que son grupos de expertos multidisciplinarios integrado por profesionales de diferentes disciplinas (economistas, sociólogos, miembros del servicio de Relaciones Exteriores, tecnólogos, políticos, militares, y otros) que aportan conocimientos específicos. En algunos casos, estos servicios son encargados a instituciones públicas o privadas, tal como universidades, centros de estudio, y similares.

Merece recordarse que la estructura de inteligencia estratégica trabaja exclusivamente "...para servir únicamente a su 'Cliente' o 'Consumidor(es)'. El cliente es el que necesita la información para tomar decisiones, usualmente es el Presidente, y algunos colaboradores cercanos como los Ministros. Sólo a él o a ellos..."<sup>665</sup> Por ello la tarea del analista es trascendente en la medida que proveerá al decisor de más alto nivel del Estado un producto que es indispensable, cual es el conocimiento necesario para la comprensión de su entorno, el ajuste de su estrategia, la adopción de medidas de intervención e influencia en la realidad y el desarrollo de operaciones de información y desinformación y de contrainteligencia en el terreno de la seguridad y la defensa nacional.<sup>666</sup>

Pasan por las manos de los analistas requerimientos sobre temas disímiles, tales como asuntos relativos a la política nacional e internacional, la competencia política y económica entre los países, educación, estrategia, el avance tecnológico, los problemas medioambientales, los delitos, la energía, la exploración científica y espacial, la investigación operativa, los conflictos, las

## Gestión de Inteligencia en las Américas

sustancias peligrosas, las amenazas a la seguridad nacional, los medios de transporte, infraestructura crítica, la producción agraria, y muchos otros, así como también todas las concepciones del desarrollo tecnológico destinadas a obtener, almacenar y procesar el “quantum informativo” requerido por la decisión al más alto nivel. Estos son algunos de los sumamente extensos ámbitos de injerencia propios del analista de inteligencia estratégica, y por ellos las cualidades académicas que requieren deben ser sobresalientes.

En su labor, el analista de inteligencia, deberá

observar el trasfondo de los sucesos, revisar en profundidad los grandes temas del país y el mundo, rescatar de la historia todo aquello que conserve vigencia, descubrir tendencias, definir nuevas líneas de aproximación a los interrogantes sin explicación, descorrer el velo engañoso de las interpretaciones simplistas, bosquejar el posible futuro.<sup>667</sup>

El conocimiento y la inteligencia, no pueden generarse mediante herramientas tecnológicas. La información se busca y se gestiona; el conocimiento se crea<sup>668</sup> y esta es una labor eminentemente humana e insustituible, puesto que no existen herramientas tecnológicas para la gestión del conocimiento que lo suplanten. En todo caso, las herramientas existentes sólo pueden ser comprendidas y utilizadas en el marco del contexto que imponen la planificación y los métodos y técnicas de la gestión del conocimiento.<sup>669</sup> Por ello, el gran valor de los analistas de inteligencia radica en sus capacidades intelectuales, su conocimiento tácito acumulado y el dominio de las herramientas de auxilio técnico.<sup>670</sup>

Por ello es que resulta indispensable la adecuada formación y capacitación del profesional dentro del más alto nivel educativo, a fin que adquiera el dominio del método científico de investigación, la pericia en los procesos de pensamiento analítico riguroso ajustados a métodos estrictos de razonamiento y análisis para avanzar en la profundización de conocimientos, el manejo de herramientas de abordaje que le permitan comprender y desentrañar la trama oculta y recóndita de la realidad, así como las habilidades para aplicar los procedimientos e instrumentos propios de la gestión del conocimiento, todo lo que, junto a la competencia personal, habilidad creativa y juicio inteligente, darán como consecuencia el resultado deseado.



## Educación superior y excelencia educativa

Dentro del marco de la educación superior, el postgrado es la última fase de la educación formal, es el máximo nivel educativo al que puede acceder un graduado universitario. Este es el terreno desde donde se promueve la formación de especialistas y expertos, o sea de donde surgen los recursos humanos vitales para el desarrollo de un país, y por tanto resulta ser también más apropiado para el profesional de la inteligencia estratégica, en la medida que implica el desarrollo de un proceso sistemático, selectivo y altamente exigente. Es el espacio académico en el que se propicia las actividades de creación intelectual en el campo científico, tecnológico y humanístico, y por consiguiente, desde donde se genera el conocimiento trascendente.

Este elevado nivel educacional, se caracteriza por la realización de un conjunto de procesos de formación que se orientan a la producción de conocimiento, -lo que se logra a través de la elaboración intelectual propia de la investigación científica-, dando como resultado el surgimiento de teorías e innovación tecnológica, cumpliendo además con las necesidades de especialización o actualización profesional a través de tres categorías académicas reconocidas en los sistemas de educación formal: la Especialización, la Maestría (o Master) y el Doctorado.<sup>671</sup> Esta clasificación es relativamente uniforme en casi todos los sistemas educativos de América,<sup>672</sup> y si bien el Diplomado no integra esta categoría académica, estos estudios deben ser considerados en mérito al prestigio de la institución que lo otorga, a la calidad académica del programa de estudios y a sus exigencias.

La conducción de la estructura académica requiere saber del funcionamiento de los procesos educativos, continuado ejercicio del profesorado universitario, haber dirigido programas educativos, probada investigación académica, conocimientos de gestión institucional y poseer títulos de educación superior acordes con su función. Es deseable que conozca las necesidades, saberes, perfil profesional, técnicas específicas y todo aquello necesario para la formación y capacitación de un profesional de la inteligencia. Igualmente toda la estructura directiva, docente y técnico-administrativa del centro de estudios debe poseer un nivel de idoneidad suficiente.

No resulta aceptable la participación de profesores empíricos y la inexistencia de una planta docente profesional y estable, y menos aún que esto sea

## Gestión de Inteligencia en las Américas

suplido por la anárquica participación de conferencistas, o por una serie de cursos y seminarios inconexos en términos de una preferida continuidad curricular y cognitiva. Este tipo de inconsistencias revela la falta de currículo, la carencia de planes de estudios estables, y exhiben un voluntarismo propio de una burocracia profana en el conocimiento de la gestión de los procesos educativos.

En muchos países, los centros de enseñanza que asumen la formación profesional de los recursos humanos de inteligencia no adhieren a los postulados de la educación formal de su país, no son instituciones educativas acreditadas, y no tienen títulos reconocidos por el sistema educativo al que deberían pertenecer. La institución educativa que carece de mecanismos de control y evaluación adecuados se ve perjudicada en la calidad de los procesos de enseñanza/aprendizaje y sus resultados; ven afectados los procesos de producción y transferencia de conocimientos; les impide mejorar la calidad del sistema en cuanto a su articulación e integración con relación a las demandas y necesidades reales; y la limita en cuanto a la calidad institucional y la solidez de las capacidades y mecanismos de gestión sobre sus distintos procesos.

La falta de una "cultura de evaluación institucional" en las entidades educativas, hace prevalecer una racionalidad interna de auto-reproducción, basada en decisiones burocráticas y corporativas, que menoscaba el proceso de educación, y deja la institución sin un juicio externo respecto a los fines, eficacia y eficiencia, capacidad, pertinencia, y calidad de los servicios y actividades. Por otra parte, los mecanismos estatales de asignación de recursos continúan operando frecuentemente en forma inercial y automática, manteniendo los subsidios a la oferta tradicional de servicios, sin una vinculación de la provisión de recursos anualmente con la "responsabilidad formal", la calidad, el desempeño, la productividad, y los resultados.<sup>673</sup>

### Estructuras de educación en inteligencia en la región

Pareciera que los conceptos expresados sobre calidad académica podrían resultar difíciles de alcanzar, pero hay numerosas alternativas que permiten lograr una educación de excelencia y obtener un profesional de gran aptitud para su tarea. De hecho, algunos países han considerado la educación superior como la alternativa más adecuada en los esfuerzos por la profesionalización de su personal.<sup>674</sup>

Se pueden identificar tres tendencias en la forma de realizar la educación profesional: 1) la organización de inteligencia realiza la educación profesional a través de su propia estructura académica, en forma autónoma, 2) la organización de inteligencia posee su propia estructura académica, pero parte de la gestión educativa la realizan centros académicos externos, y 3) la organización de inteligencia pone en manos de una estructura académica externa la ejecución de la totalidad del proceso educativo. En este caso, puede tratarse de una universidad o de un centro de estudios de las fuerzas armadas.

A continuación se presentan las diferentes formas elegidas por algunas de las organizaciones de inteligencia del continente, para dar respuesta a sus necesidades de educación para el profesional de la inteligencia estratégica, donde se podrán percibir las importantes diferencias en cuanto a su estructuración, nivel académico y calidad educativa. Asimismo, a través de la tabla presentada como Anexo 1, se podrán verificar las principales diferencias en cuanto a las características de los centros de formación civiles y militares, así como si se tratan de centros acreditados, de postgrado y si su acceso se encuentra abierto a civiles.

#### a. ARGENTINA

En Argentina, la Secretaría de Inteligencia, posee como órgano educativo a la Escuela Nacional de Inteligencia (ENI). Se ha optado por un sistema mixto por el que la ENI, a través de un convenio con la Universidad Nacional de La Plata, brindan en conjunto el Magister en Inteligencia Estratégica Siglo XXI.<sup>675</sup> Está inserto en el sistema de educación superior nacional y tiene por objetivo principal otorgar a los graduados una formación compuesta de conocimientos generales, específicos e interdisciplinarios y habilidades metodológicas necesarias para su aplicación en diversas áreas del conocimiento y del quehacer público o privado. Su oferta académica es abierta a todos los interesados sean o no pertenecientes a la comunidad de inteligencia. Desde el 2013 el convenio ENI - Universidad de la Plata se encuentra suspendido.

La Ley Nacional de Inteligencia del 2001 (Ley 25520) ha propiciado el crecimiento académico de la estructura educativa de inteligencia dentro del sistema educativo nacional, así, el artículo 29 dispone que los estudios cursados en la ENI podrán ser objeto de convalidación por parte del Ministerio de Educación de la Nación, conforme a las leyes y reglamentaciones vigentes.

## Gestión de Inteligencia en las Américas

También, a través del artículo 30, se impulsa el relacionamiento y la colaboración institucional con universidades y centros de estudios.

El Instituto de Inteligencia de las Fuerzas Armadas (IIFA), una institución conjunta que depende del Estado Mayor Conjunto, también posee una carrera acreditada -una especialización en análisis estratégica- la cual se ofrece a aspirantes civiles tanto como militares.

### b. BOLIVIA

La Dirección de Inteligencia del Estado (DIE) es el organismo de inteligencia estratégica de Bolivia, con personal primariamente militar, con participación de civiles, y si bien carece de una institución educativa de ese nivel, la Escuela de Inteligencia del Ejército es la que provee la capacitación de la mayor parte del recurso humano.

La Escuela Militar de Inteligencia del Ejército “Gral. De Ejército Joaquín Zenteno Anaya” posee como oferta académica el Diplomado en Inteligencia Estratégica y el Diplomado en Información Estratégica. Están dirigidas a formar personal profesional militar, policial y civil, orientadas a capacitar para quienes tienen a cargo la tarea de asesorar en los procesos de decisión de organizaciones e instituciones públicas y privadas a través de la producción de información e inteligencia estratégica, utilizando métodos de análisis prospectivos y diversas técnicas de análisis de información y datos.

Asimismo, la Escuela de Comando Estado Mayor del Ejército “Mariscal Andrés de Santa Cruz”, dicta una Maestría en Inteligencia Estratégica, dirigida a civiles y militares. Su objetivo es proporcionar los conocimientos y capacidad de participar en el análisis y producción de la inteligencia estratégica y asistencia a los responsables en los diferentes niveles con una visión integradora y trascendente en el ámbito de la defensa y seguridad nacionales.

### c. BRASIL

La *Agência Brasileira de Inteligência* (ABIN) posee su propio elemento de educación, la *Escola de Inteligência* (ESINT) -continuadora de la Escola Nacional de Informações (EsNI)-, es quien tiene la responsabilidad de preparar funcionarios públicos de la administración pública de nivel federal y estadual integrados en el *Sistema Brasileiro de Inteligência* (SISBIN), civiles y militares,

para responder a las necesidades de inteligencia del sistema nacional a través de programas específicos de entrenamiento, cursos y seminarios.

También la *Escola Superior de Guerra, dicta el Curso Superior de Inteligência Estratégica* (CSIE), dirigido a preparar a civiles y oficiales superiores de las fuerzas armadas para cumplir funciones de inteligencia estratégica en los organismos de la administración nacional vinculados al SISBIN.

#### d. CHILE

En Chile no hay una institución educativa dentro de la Agencia Nacional de Inteligencia (ANI), por ello es que la formación del personal se realiza a través de universidades e instituciones educativas de las fuerzas armadas.

Varios programas han sido desarrollados en Chile desde fines de la década de los 1990, algunos han quedado discontinuados, y otros se han integrado a otras carreras relacionadas a la defensa y a la seguridad, donde subsisten los estudios sobre temas de inteligencia.

Hasta el año 2009, la Universidad de Chile, a través del Departamento de Ciencia Política del Instituto de Asuntos Públicos, desarrolló un programa de Diploma Metodología de Análisis en Inteligencia Estratégica, cuyo objeto era formar profesionales capacitados para asesorar los procesos de toma de decisión en organizaciones e instituciones públicas y privadas a través de la producción de inteligencia estratégica. Estaba dirigido a profesionales, estudiantes de último año de una carrera universitaria, personal de instituciones de militares y policiales o pertenecientes a las áreas de análisis y/o inteligencia.

También la Academia de Guerra del Ejército (ACAGUE) desarrolló un programa de Magister en Ciencias Militares con Mención en “Inteligencia Estratégica” organizado en tres etapas. La primera, en común con los estudios del programa de Ciencias Militares. La segunda etapa era cumplida en la Universidad de Chile, otorgándose un Diploma de Inteligencia Estratégica. Cumplidas ambas etapas, se da inicio al trabajo tutorial y de elaboración de la Tesis.

Ya que el programa de la Universidad de Chile está en hiato, junto con el de ACAGUE, actualmente la Academia Nacional de Estudios Políticos y Estratégicos (ANEPE) -institución de educación superior dependiente del Ministerio de Defensa Nacional-, dicta el Diplomado “La Función Inteligencia en

## Gestión de Inteligencia en las Américas

el Estado Contemporáneo”, siendo su objetivo colaborar con la formación de una cultura nacional de inteligencia y mostrar la importancia que esta tiene en la sociedad.

Es importante tener en consideración que las experiencias educativas chilenas ya sea en instituciones oficiales o universidades, han sido útiles a los fines de la profesionalización y ha generado el interés de la comunidad académica, conformándose en ese ámbito un importante núcleo de producción intelectual.

### e. COLOMBIA

La educación en inteligencia ha sido una tarea de la Academia Superior de Inteligencia y Seguridad Pública, dependiente del Departamento Administrativo de Seguridad (DAS), con cursos específicos y especializaciones dictadas en sus escuelas. Sin embargo, su calidad educativa ha sido objeto de críticas e incluso, el “Informe de la Comisión Especial para el DAS” de marzo de 2006 ha realizado observaciones respecto de su currículo, de la falta de calidad en su profesorado, la necesidad de adopción de procesos de evaluación externa, entre otras recomendaciones.<sup>676</sup>

A fines del 2011, el DAS fue reemplazado por la Agencia Nacional de Inteligencia, quedando por tanto indefinida la suerte de la Academia.

Por otra parte, el Ejército de Colombia tiene la Escuela de Inteligencia y Contrainteligencia “BG Ricardo Charry Solano” (ESICI). Es una institución universitaria con reconocimiento oficial del Ministerio Nacional de Educación de Colombia desde el 2002 y mantiene su acreditación mediante procesos de autoevaluación y de evaluación institucional. Su finalidad es la de formar, capacitar, especializar y reentrenar al personal de las Fuerzas Militares, civiles, organismos del estado a nivel nacional e internacional, en inteligencia, con el fin de atender las necesidades institucionales. La ESICI dicta una Maestría en Inteligencia Estratégica y Prospectiva así como también Especializaciones y Diplomados en diferentes temas de la especialidad, y se encuentra entre sus planes desarrollar programas de maestrías y doctorado.<sup>677</sup>

También la Universidad Militar Nueva Granada, posee un Diplomado en Inteligencia Estratégica dirigido a funcionarios del sector privado y público, miembros de las Fuerzas Militares, de la Policía Nacional en actividad y retiro,

integrantes de los cuerpos de seguridad del Estado, estudiantes universitarios, sectores académicos y en general a interesados en el estudio y análisis de los factores estratégicos.

#### f. ECUADOR

En el año 2009, con la Ley de Seguridad Pública y del Estado y el Decreto 1768, se crea la Secretaría Nacional de Inteligencia (SENAIN) dependiente de la Presidencia de la Nación. Es el órgano rector del Sistema Nacional de Inteligencia, produce y proporciona inteligencia político-estratégica en forma permanente y oportuna para el nivel político de decisión, con el fin de prevenir y neutralizar los riesgos y amenazas que atenten la Seguridad Pública y del Estado. Si bien está entre sus planes el establecer una nueva Escuela de Inteligencia para la capacitación de sus miembros, en la actualidad, la mayor parte del personal proviene de centros de formación y capacitación de inteligencia militar.

#### g. ESTADOS UNIDOS

Estados Unidos posee numerosas instituciones educativas que tienen oferta académica sobre Inteligencia Estratégica ya sean pertenecientes a las diversas agencias del Estado civiles y militares, como así también universidades.

En agosto de 2011 inicia sus actividades la Universidad Nacional de Inteligencia, (National Intelligence University) creada a partir de la estructura del *National Defense Intelligence College* (NDIC).<sup>678</sup> Es una institución de educación superior y de investigación y tiene por fin la preparación de los miembros de la comunidad de inteligencia, miembros de las fuerzas armadas y de empleados federales de la estructura de Seguridad Nacional. Posee autorización del Congreso de los EE.UU. para expedir títulos universitarios y se encuentra acreditada ante *The Middle States Association of Colleges and Schools*. Entre los numerosos programas que se desarrollan, se destacan: Licenciatura en Ciencias de Inteligencia (BSI), Maestría en Ciencias de Inteligencia Estratégica (MSSI), Maestría en Ciencia y Tecnología de Inteligencia (MSTI).

La Agencia Central de Inteligencia (CIA) tiene a su cargo el *Center for the Study of Intelligence*, que es una institución educativa profesional que tiene por finalidad promover el estudio, el debate y la comprensión del rol de la inteligencia en la sociedad norteamericana. Entre las extensas actividades

## Gestión de Inteligencia en las Américas

académicas que desarrolla para la difusión de la inteligencia, edita la revista *Studies in Intelligence* que fuera fundada por Sherman Kent en 1955.

Junto con las instituciones educativas de inteligencia oficiales, se encuentran numerosos centros de estudios que se dedican a ofrecer programas de educación superior en temas de inteligencia estratégica, tal el caso de *Loyola University of Maryland*, *Mercyhurst University* (de Erie, Pennsylvania), *Institute of World Politics* o del *Naval Postgraduate School*.

### h. GUATEMALA

La Ley Marco del Sistema Nacional de Seguridad, Decreto Numero 18-2008, surge con el objeto de establecer las normas jurídicas de carácter orgánico y funcional necesarias para la realización coordinada de las actividades de seguridad interior, exterior y de inteligencia por parte del Estado de Guatemala.

Crea además el Consejo Nacional de Seguridad y bajo su dependencia, al Instituto Nacional de Estudios Estratégicos en Seguridad que es la estructura orientada a formar, profesionalizar y especializar el recurso humano idóneo, mediante la dirección y coordinación de diferentes instituciones de enseñanza del Estado en materia de seguridad, impulsando programas de diplomados, licenciaturas, maestrías y doctorados. Su tarea es la de garantizar la excelencia profesional en el ejercicio de la función del personal y la igualdad de oportunidades para el ingreso y ascenso, y de establecer el sistema de carrera profesional de todos los organismos que conforman el Sistema Nacional de Seguridad.

La Secretaría de Inteligencia del Estado (SIE), es una estructura vinculada al Consejo Nacional de Seguridad que forma parte del Sistema Nacional de Seguridad, y por tal razón el Instituto Nacional de Estudios Estratégicos en Seguridad participa en la formación y capacitación del personal de inteligencia. A su vez el Acuerdo Gubernativo Número 413-2008, dicta el Reglamento Orgánico de la Secretaria de Inteligencia, creando en el Capítulo III, Artículo 46, la Unidad de Capacitación y Becas, órgano administrativo encargado de formar y promover la capacitación permanente del personal profesional, técnico y administrativo de la SIE. La Unidad también tiene a su cargo la elaboración del plan estratégico para la capacitación del personal de la Secretaria.



## i. MEXICO

A partir de la década del los 1980 algunas instituciones del ámbito militar como el Colegio de la Defensa y Centro de Estudios Superiores Navales incursionaron en la enseñanza de la inteligencia desde la temática de la Defensa Nacional. El Centro de Investigación y Seguridad Nacional (CISEN) institución civil creado en 1989, tomó a su cargo la formación y capacitación del personal de inteligencia, mediante el Curso en Defensa Nacional y el Programa en Estudios Estratégicos, junto a una innumerable cantidad de diplomados, cursos, talleres y seminarios (que en muchos casos nada tienen que ver con la especialidad<sup>679</sup>) para personal de la institución y de otros organismos del Estado, conformando una oferta educativa verdaderamente anárquica.

La profusa oferta académica resultó insuficiente e inadecuada para cubrir las necesidades del CISEN, y como revela Guillermo Valdez Castellanos,

los investigadores y analistas requieren de una formación especializada en inteligencia y contrainteligencia y en México no existe ninguna escuela que ofrezca ese tipo de formación; incluso la materia de seguridad nacional es prácticamente desconocida en las universidades del país. La cultura de seguridad nacional en México está en pañales. Lo anterior significa que el Centro tiene que ser autosuficiente en la formación de su personal.<sup>680</sup>

Así es que se comienza a pensar en la posibilidad de crear una nueva estructura educativa que satisfaga las necesidades del CISEN.

El 16 de abril de 2009, es publicado en el Diario Oficial de la Federación el “Acuerdo por el que se crea la Escuela de Inteligencia para la Seguridad Nacional del Centro de Investigación y Seguridad Nacional (ESISEN)”, estructura educativa que depende del Centro de Investigación y Seguridad Nacional (CISEN). La norma de creación la define como una institución educativa con capacidad académica en materia de inteligencia civil para la seguridad nacional. Establece también que impartirá los planes y programas de estudios aprobados por la Secretaría de Educación.

Si bien inicialmente la convocatoria de ingreso está dirigida a las entidades gubernamentales relacionadas con la inteligencia y la seguridad nacional, está

## Gestión de Inteligencia en las Américas

prevista la apertura de su oferta académica al público general. La ESISEN busca promover los estudios, la reflexión y la cultura sobre temas de inteligencia y seguridad nacional, tanto al interior de las instituciones gubernamentales como entre la ciudadanía. A través de los recursos técnicos del CISEN se pondrán a disposición de estudiosos e interesados externos referencias bibliográficas, documentos y otros materiales no reservados que puedan contribuir a este propósito.<sup>681</sup>

Es importante señalar que el Instituto Tecnológico de Monterrey, posee desde el 2008 en su Escuela de Graduados en Administración Pública y Políticas Públicas (EGAP), una Cátedra de Investigación en Inteligencia Estratégica, que tiene como objetivo desarrollar y estudiar conceptos y metodologías en el área de inteligencia, desarrollar y establecer una estrategia de difusión en el área así como promover la adopción e institucionalización del conocimiento generado. En el marco de dicha Cátedra se desarrolla el Curso de Desarrollo y Administración de Sistemas de Inteligencia Estratégica, y también se realiza investigación y publicaciones.

### j. PARAGUAY

En Paraguay, la Dirección de Inteligencia (DI) del Ministerio del Interior y la Dirección de Política y Estrategia (DIE) del Ministerio de Defensa, son las estructuras que tienen responsabilidades en materia de Inteligencia Estratégica. El personal de ambas estructuras es formado principalmente en instituciones educativas de inteligencia de las fuerzas armadas.

El Instituto de Altos Estudios Estratégicos (IAEE) tiene a su cargo el desarrollo del Curso de Inteligencia Estratégica (CIE), concebido como un diplomado de especialización. El IAEE es una institución de educación superior del sector público dependiente del Ministerio de Defensa Nacional, que desarrolla especializaciones y maestrías en temas relativos a la defensa nacional. El Curso de Inteligencia Estratégica está dirigido al personal de las fuerzas armadas, a la comunidad de inteligencia y líderes de la conducción del Estado. Se orienta a lograr el eficaz desempeño del personal en las funciones asignadas dentro de las agencias u organismos de inteligencia.

La estructura docente del CIE está conformada por un grupo de instructores del Ejército Argentino, -provistos por el programa de cooperación con

el Ministerio de Defensa de la República Argentina- que participan junto a conferencistas de diversas instituciones oficiales paraguayas tales como la Fiscalía Antisecuestros, la Secretaría de Prevención de Lavado de Dinero (SEPRELAD), el Departamento Técnico Aduanero de Vigilancia Especial (DETAVE), la Comisión de Derechos Humanos, entre otras.

#### **k. PERU**

En el caso de Perú, la Dirección Nacional de Inteligencia tiene dentro de su estructura a la Escuela Nacional de Inteligencia (ENI) y en ese ámbito se desarrollan los cursos y seminarios de diversos niveles en materia de inteligencia. En esta institución se realiza el Curso Superior de Inteligencia Estratégica, que tiene a su cargo la capacitación de funcionarios de la Dirección y del Sistema Nacional de Inteligencia, así como de diferentes organismos públicos. Es interesante notar que la Reglamentación de la Ley N° 28664 que regula el Sistema Nacional de Inteligencia, establece en el Artículo 23° que para ser nombrado Director de la Escuela Nacional de Inteligencia se debe poseer el grado académico de maestría.

A su vez, el Centro de Altos Estudios Nacionales (CAEN) dicta un Diplomado en Inteligencia Estratégica que está dirigido a políticos, funcionarios del sector público, empresarios, profesionales, militares, policías y agregados militares. El CAEN es la Institución de perfeccionamiento del más alto nivel del Sistema Educativo del Sector Defensa del Perú, depende de la Dirección General de Política y Estrategia del Ministerio de Defensa. Es una institución de enseñanza superior de postgrado y otorga títulos de Especialización, de Magister y Doctor en temas de Defensa.

También el Instituto Peruano de Políticas Públicas, a través de un convenio con la Universidad Nacional Mayor de San Marcos, desarrolla el programa de Especialización en Inteligencia Estratégica y Democrática, dirigido a profesionales, estudiantes de último año de una carrera universitaria, personal de instituciones militares, policiales o que trabajen en las áreas de análisis y/o inteligencia.

#### **I. ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA)**

A pesar de tratarse de una organización internacional, la OEA a través de la Comisión Interamericana para el Control del Abuso de Drogas (CICAD),

## Gestión de Inteligencia en las Américas

-órgano dependiente de la Secretaría de Seguridad Multidimensional (SSM)-, posee un programa educativo para formar expertos en inteligencia estratégica. Las actividades se desarrollan mediante la Escuela Regional de la Comunidad Americana de Inteligencia Antidrogas (ERCAIAD), antes llamada Escuela Regional Andina de Inteligencia Antidrogas, que fuera fundada en 1999. Este centro especializado de la CICAD tiene sede en Bogotá, y su finalidad es el de proporcionar entrenamiento académico en inteligencia estratégica y operacional, orientado al campo de la inteligencia anti-drogas, siendo los participantes provenientes principalmente de servicios de inteligencia, policía, y otras instituciones involucradas en la lucha contra el tráfico de drogas en los países del Grupo de Inteligencia Andina -Bolivia, Brasil, Chile, Colombia, Ecuador, Perú y Venezuela-, así como otros los países de habla hispana miembros de la OEA.

La actividad académica se centra en cursos y seminarios de entrenamiento sobre inteligencia estratégica y operacional, que se llevan a cabo en diferentes países americanos y son desarrollados por expertos provenientes de Canadá, Francia, Alemania, España, Suecia y Estados Unidos, así como de los países miembros de la OEA y de organizaciones internacionales como INTERPOL y UNODC. En ese ámbito se desarrolla el Curso de Inteligencia Estratégica: Estructura lógica de análisis y prospectiva del narcotráfico en el hemisferio al 2020. Su programa ha tenido un proceso de evaluación académica independiente, dando como resultado que su calidad académica es la adecuada.

### m. URUGUAY

La Dirección Nacional de Inteligencia de Estado, institución perteneciente al Ministerio de Defensa de Uruguay, no posee estructura de educación de su dependencia, realizándose la formación del personal en el ámbito militar.

El Instituto Militar de Estudios Superiores perteneciente al Ejército Nacional Uruguayo, integrando el Sistema de Enseñanza del Ejército, desarrolla un Curso de Inteligencia Estratégica. Está dirigido a Personal Militar Superior en actividad con Curso de Estado Mayor o Curso Básico Inteligencia, funcionarios de la Dirección Nacional de Inteligencia de Estado y personal que cumpla tareas en Organismos de Inteligencia de Estado. Este centro de estudios, desde el año 2001 tiene reconocimiento oficial como institución universitaria.

También, el Centro de Altos Estudios Nacionales (CALEN) dependiente del Ministerio de Defensa, tiene previsto iniciar en el transcurso del año 2012 un Curso de Inteligencia Estratégica,<sup>682</sup> dirigido a la formación de analistas de la comunidad de inteligencia local. La iniciativa está orientada a que este curso forme parte de un conjunto de actividades académicas que permitan acceder a una Maestría en Defensa Nacional.

#### n. VENEZUELA

El Decreto 7453 del primero de junio de 2010, crea el Servicio Bolivariano de Inteligencia Nacional (SEBIN). Es un organismo de inteligencia y contrainteligencia interior y exterior de naturaleza civil, que depende del Ministerio del Poder Popular para el Interior y Justicia. Posee como estructura académica al Centro de Estudios de Inteligencia (CEI), y tiene por misión diseñar, planificar, ejecutar y supervisar las actividades y programas de formación, capacitación, actualización, adiestramiento en servicio y especialización con el fin de garantizar la formación integral de acuerdo a los objetivos funcionales en materia de inteligencia y contrainteligencia. Se centra en cursos de nivel básico y son sólo para su personal, aunque gran parte de la capacitación de sus funcionarios es mayormente realizada a través de la estructura educativa de las fuerzas armadas.

El Ministerio del Poder Popular para la Defensa desarrolla mediante la Universidad Militar Bolivariana de Venezuela (UMBV),<sup>683</sup> cursos de diferentes niveles en materia de inteligencia militar, dirigidos a personal militar y miembros de los cuerpos de seguridad del Estado. La universidad cuenta con la Escuela de Guerra Conjunta de las Fuerzas Armadas Bolivarianas (antes Centro de Estudios Avanzados Militares), la Escuela de Inteligencia y Operaciones Psicológicas de las Fuerzas Armadas Bolivarianas “G/B Daniel Florencio O’Leary”, y el Instituto de Altos Estudios de la Defensa Nacional “Gran Mariscal de Ayacucho Antonio José de Sucre” (IAEDEN), realizándose en estas instituciones estudios relacionados principalmente con temas de seguridad y defensa.

El análisis de las estructuras educativas de inteligencia de la región, muestra diferencias en cuanto a sus modalidades y capacidades, y si bien en algunos casos han optado por alternativas de calidad académica, resulta difícil determinar en forma estricta la excelencia de su resultado. En tal sentido para establecer la calidad académica del profesional obtenida en la gestión de

## Gestión de Inteligencia en las Américas

enseñanza/aprendizaje, se requiere de un proceso de evaluación, que con bases científicas, permitirá establecer el nivel de la educación obtenida por el recurso humano. Por lo antes expresado se ha considerado conveniente presentar a continuación, un modelo de proceso de evaluación académica del personal de una estructura de inteligencia gubernamental, que en forma ilustrativa sirva de guía de aplicación en las organizaciones de la región.

### Proceso de evaluación de la calidad de formación académica del recurso humano en inteligencia

El proceso de evaluación es un procedimiento técnico conformado por normas y objetivos sumamente precisos, que permite tener una clara idea del funcionamiento institucional en toda su gestión, de sus capacidades, sus fortalezas y debilidades y de las mejoras que deben realizarse en aspectos técnicos, procedimentales, y de personal, a fin de alcanzar los objetivos deseados. Es una tarea que deberá realizarse dentro de la organización en forma permanente y exhaustiva.

La organización debe poseer un plan de evaluación institucional, -del que deriven planes operativos-, que permita orientar en cuanto a los objetivos, que sirva para establecer que es lo que se debe evaluar, quien evalúa y a quienes, que determine qué tipo de información se debe coleccionar en el proceso, que defina el motivo de la evaluación, la construcción de indicadores, el establecimiento de criterios de evaluación, la recolección de datos y su valoración, la forma de obtener los productos de la evaluación y como aprovecharlos, así como las pautas para elaborar el informe, su difusión, y los mecanismos para la instrumentación de un proceso de cambio si correspondiera.

Un aspecto importante en todas las organizaciones es la de determinar la calidad y eficiencia del recurso humano que posee. Algunos indicadores de éstas son la forma en la que desempeña su trabajo y su nivel educativo, así como sus cualidades y capacidades, posibilitando un apropiado proceso de toma de decisiones en diversos aspectos de la política de personal de la organización, en especial en cuanto a los cambios necesarios en el comportamiento, las destrezas o los conocimientos que se requieren para su función. En la gestión del personal la evaluación proporciona previsibilidad, permitiendo elaborar planes para el mejor aprovechamiento de los recursos humanos, proveyendo criterios para la mejora del rendimiento y calidad laboral.

La evaluación del recurso humano, también permite identificar los requerimientos académicos de la organización, por cuanto sus resultados podrán servir para establecer las reales necesidades de formación, capacitación, adiestramiento y entrenamiento del personal, pero para que sea válido, representativo y útil se debe incluir en el proceso a todos los profesionales de la organización. Esta tarea puede realizarse a través de diferentes métodos, aplicando técnicas e instrumentos tales como el empleo de tests psicométricos, muestras de trabajo, procedimientos de observación, entrevistas, cuestionarios o cualquier otro procedimiento de recogida de datos, debiéndose emplear aquellos que resulten más confiables para obtener un resultado relevante, veraz, estable, verificable, cotejable y confrontable.

Es posible desarrollar un modelo genérico para ejemplificar como debería ser un proceso de evaluación académica de la institución que permita establecer el grado de influencia de la educación en la calidad del profesional. Para esto habrá que tener en cuenta en la estrategia de evaluación la necesidad de considerar un elemento objetivo -como son títulos académicos y de capacitación del profesional-, y relacionarlo con apreciaciones basadas en su trabajo tales como aplicación de conocimientos, calidad, eficiencia, y capacidad de análisis. Esto permitirá determinar -en el marco de un estudio individual y de conjunto- si existe una relación real entre el nivel educativo con el resultado de la labor profesional.

A tal fin, se puede desarrollar este proceso ilustrativo -que se presenta en forma sucinta, simplificada y a modo de prototipo- en base a la aplicación de cuatro estrategias de evaluación: a. Evaluación curricular, b. Evaluación del desempeño laboral, c. Evaluación personal por entrevista y d. Evaluación de conocimientos.



**Figura 12.** Esquema del Proceso Evaluación Académica de la Institución

**Fuente:** Creado por el autor.

Las características de las estrategias de evaluación elegidas para este ejemplo son las siguientes:

- a. La evaluación curricular permite establecer el nivel académico y de capacitación del profesional, considerando los distintos niveles académicos que ha alcanzado en su proceso educativo. Para ello, a través de escalas, se evalúan los conocimientos, aptitudes, prácticas, técnicas y habilidades acreditadas con los títulos, grados, diplomas, certificados y constancias de capacitaciones realizadas, que guarden relación con las funciones que desempeña, valorizando cada una de ellas con un puntaje. Así, por ejemplo debería confeccionarse una hoja de evaluación (ver Anexo 2) con una tabla que permita establecer los factores de evaluación y las escalas asignadas, lo que arrojará un puntaje parcial y la suma de estos dará un resultado final de esta etapa.



b. La evaluación del desempeño laboral, permite examinar las tareas de los funcionarios, estableciendo destrezas en su desempeño así como la calidad y éxito de sus resultados. Los factores a considerar en la evaluación de desempeño están en relación con los objetivos de la evaluación, teniendo en cuenta factores institucionales, individuales y de rendimiento. Esta tarea puede ser efectuada por el jefe inmediato o supervisor, a través de un análisis de puesto, y cada uno de los campos analizados debe ser valorizado con un puntaje, que quedará plasmado en una hoja de evaluación (ver Anexo 3).

c. La evaluación personal por entrevista sirve para comprobar el grado de conocimientos en las funciones que desempeñan los miembros de la organización, así como también se puede verificar su rendimiento en relación con el nivel académico alcanzado, y en el plano profesional-institucional es posible determinar si existe una vinculación entre sus logros académicos y su evolución dentro de la estructura a la que pertenece. Esta tarea se realiza a través de una entrevista y mediante un formulario que estará dividido en dos secciones, una correspondiente a la guía de la entrevista y otra de evaluación. El entrevistador deberá determinar la importancia de cada factor con respecto a las exigencias del trabajo y documentar su opinión, considerando las impresiones y los puntos más importantes de la información obtenida durante la entrevista, expresando sus comentarios, así como las cualidades notables y puntos débiles, todo lo que deberá ser consolidado en un resumen de evaluación (ver Anexo 4).

d. La evaluación de conocimientos tiene por objeto establecer el grado de conocimientos básicos, generales y específicos vinculados a las funciones que le son propias. Se puede efectuar a través de un test o cuestionario y permite indagar sobre cuestiones vinculadas a la organización, los métodos y técnicas empleadas en su trabajo, así como una amplia gama de conocimientos que se supone el profesional debe manejar en su tarea cotidiana. La ventaja del cuestionario es que puede ser realizado por escrito, insume relativamente poco tiempo y puede abarcar gran número de personas. Para ello, es necesario que su diseño sea elaborado de manera que permita obtener respuestas correctas e información útil para su posterior valoración (ver Anexo 5).

## Gestión de Inteligencia en las Américas

Para establecer las conclusiones finales del proceso, el resultado logrado de las distintas etapas de la evaluación -curricular, del desempeño laboral, de la entrevista personal y de la evaluación de conocimientos-, deberá ser homogenizado a través del puntaje y catalizado mediante un criterio de valorización<sup>684</sup> de los puntajes obtenidos en los distintos instrumentos, los que consolidados en el resumen de evaluación (ver Anexo 6), proporcionarán un puntaje final y la calificación final, resultando de esta operatoria una información que refleja los niveles individuales. El informe final de todo el proceso de evaluación realizado en la institución, será un cruzamiento de la información extraída de la totalidad de los elementos evaluables de todo el personal de la organización, dando como resultado un producto que permitirá apreciar a través de parámetros el grado de calidad profesional y académica del personal a nivel institucional, la relación entre el nivel académico y el rendimiento laboral, así como permitirá realizar sinnúmero de conclusiones en cuanto a aspectos del material humano que se posee, exponiendo las necesidades, limitaciones y capacidades del componente profesional.

### Conclusiones

Las organizaciones de inteligencia estratégica debe tener una constante preocupación sobre la educación del recurso humano, y conforme las características del profesional deseado, deberá fijar con claridad su política educativa para que sea ejecutada, ya sea a través de un órgano académico propio o a través de otros centros educativos.

Comparto la opinión de otro observador en cuanto a la relevancia de estructurar un elemento de educación en la organización de inteligencia, basados en el conocimiento a impartir y la forma en que se deben satisfacer sus necesidades de perfeccionamiento, capacitación, profundización y/o inducción que requieren los especialistas en inteligencia estratégica.<sup>685</sup> Esto es así puesto que es necesario que las alternativas educativas surjan de lo profundo de la estructura, y que exista la generación de un proceso innovador y multidimensional, nutrido del conocimiento, del saber, de las experiencias y vivencias de la realidad a la que pertenece, pero básicamente propio y adecuado a su realidad.

Las diferentes opciones que los organismos de inteligencia han buscado para dar solución a la educación de su personal de los países analizados, muestran

una variada gama de alternativas, en el que las más avanzadas, se encuentran dirigidas a la educación superior, cumpliendo con procesos de evaluación y acreditación académica, orientándose así a criterios de excelencia institucional.

En algunos países la influencia militar en la enseñanza de la inteligencia estratégica ha tenido su correlato en la forma de concebir la educación en los centros de formación y capacitación específicos, y muchas veces los criterios de profesionalismo organizacional son reemplazados por condiciones de grado y ascenso propias de la carrera militar. Sin embargo, en algunos casos, son centros de estudios reconocidos por el sistema de educación superior, donde los programas que se dictan son abiertos y no se encuentran limitados sólo a militares o a los miembros de la comunidad de inteligencia sino que tienen cierta amplitud para la participación de otros sectores de interés de la sociedad.

La inclusión en la universidad de los estudios de inteligencia, es considerada como un paso muy positivo para el mejoramiento de la calidad educativa de la disciplina y es adecuado para neutralizar la desconfianza en cuanto a sus contenidos académicos. En tal sentido, el especialista peruano Alberto Bolívar Ocampo, señala: “un aspecto de Inteligencia que se puede considerar muy adelantado en la región...es el dictado de cursos de Inteligencia en universidades. Esto es bastante para ‘perder el miedo’ a tratar académicamente un tema vital para la salvaguarda de los intereses nacionales de cualquier país”.<sup>686</sup>

El vínculo entre la organización de inteligencia y el medio académico es de suma importancia y debe ser fortalecido en beneficio de la institución, dado que como lo expresa Jaime Castillo Arias,

es innegable la capacidad y el potencial que disponen los centros de educación superior e investigación privada, porque la información que disponen o que puedan obtener a través de su estructura e incluso en lo particular de los expertos que en las diferentes áreas existe, constituyen un componente fundamental al momento de realizar un análisis de Inteligencia nivel estratégico. En este aspecto la importancia de estos centros, se encuentra dada por el posicionamiento alcanzado en base a la transparencia y libertad académica existente. Esto será el referente para que sea considerada la información que producen estas instituciones (o el potencial

## Gestión de Inteligencia en las Américas

de hacerlo), especialmente a través de los enlaces que dispone con otros centros universitarios o de investigación especialmente en el exterior; cabe indicar que de esta libertad académica saldrá favorecido el análisis, ya que contará con un insumo idóneo para alcanzar los resultados que permitan realizar el asesoramiento adecuado.<sup>687</sup>

La apertura de la oferta educativa y el tratamiento de las cuestiones de inteligencia en las aulas universitarias, tiene como resultado la democratización del conocimiento, haciendo que el tema de la inteligencia estratégica sea más asequible al mundo académico, permitiendo su discusión y difusión, impulsando los estudios e investigación sobre la especialidad y el desarrollo de “think tanks”, produciendo la generación y actualización de la teoría y su gemela operativa, la “doctrina”, todo lo que en definitiva permite acrecentar la cultura de inteligencia.

El personal que trabaja en el mundo de la inteligencia estratégica requiere de un amplio espectro de conocimientos, de un nivel de excelencia acorde con la alta responsabilidad y la complejidad de su tarea, por lo cual debe ser formado con solidez académica para obtener un profesional de alto rendimiento.

Por ello es importante tener en cuenta que, para que los profesionales de la inteligencia alcancen

un alto nivel de conocimiento y experticia -no medida por la cantidad de cursillos y diplomados-, deberá fomentarse una constante relación con la academia para generar un compromiso con la excelencia gracias al acceso a especializaciones, maestrías y doctorados; viejo anhelo de muchos, frustrado por las comprensibles altibajos presupuestales que han representando un lastre económico a ese proceso formativo de largo plazo y la carencia de iniciativas legislativas que den mayores oportunidades para los aspirantes a esa formación.<sup>688</sup>

La calidad del recurso humano está sujeta no sólo a las condiciones personales del individuo, sino también será producto del proceso educativo por el que haya pasado. Por esta razón, cualquiera sea la forma en que la institución educativa de inteligencia resuelva la cuestión educativa, es indispensable que

permanentemente supervise el enlace y la coherencia entre las necesidades educativas de la organización de inteligencia, la calidad y cualidades del elemento académico, los contenidos de los programas de estudio y su adecuación a los perfiles profesionales. También es necesario, realizar procesos de evaluación permanentes a fin de establecer con precisión los requerimientos institucionales en cuanto la formación, capacitación, adiestramiento y entrenamiento del personal, los niveles académicos deseables, así como numerosa información necesaria para el mejor aprovechamiento de los recursos humanos.

Pero debe recordarse que en el ámbito de la educación, -a pesar de los conocimientos y títulos académicos-, el profesional de la inteligencia siempre tendrá frente a sí dos posibilidades: la del aprendizaje continuo y permanente o la de la ignorancia gradual e irreversible. Es la organización la que en definitiva deberá encargarse de que su personal no caiga en la inercia y en el abandono intelectual y académico, porque en el mundo cambiante en el que vivimos el conocimiento pierde vigencia rápidamente y la desidia educativa conduce en poco tiempo a la ignorancia.

### Biografía del autor

**José Gabriel Paz**, J.D., Ed.M., Director del Instituto de Investigaciones en Geopolítica, Defensa y Seguridad de la Universidad del Salvador (Argentina), Director del Master en Defensa y Seguridad Hemisférica (USAL-CID, Washington DC), Director del Master en Defensa y Seguridad Centroamericana (USAL-CDN, Honduras), Profesor de las materias: “Geopolítica”, “Organismos Internacionales”, “Terrorismo Internacional” y “Amenazas Transnacionales” en la Universidad del Salvador (Argentina). Asesor del *Center for Latin American Economy and Trade Studies del Chihlee Institute of Technology* de Taiwan. Graduado de: “Curso de Postgrado de Inteligencia Estratégica” (ESG) Argentina, “Curso de Postgrado en Geopolítica” (ESG) Argentina, “Seguridad Nacional” (Galil College), Israel, “Army Instructor” (U.S. Army), EE.UU. Autor del libro, *Bases normativas para el establecimiento de la paz y la seguridad internacional, Tomo 1 y Tomo 2*, Editorial Universidad Libros (2000). Ha escrito numerosos artículos, entre ellos: “El ambiente antártico y las amenazas a la seguridad ambiental global,” *Revista de la Escuela Nacional de Inteligencia*, Buenos Aires, Vol. I, N° 1, 2003. Contacto: paz.jose@yahoo.com.

## Gestión de Inteligencia en las Américas

Anexo 1 (Tabla 16)								
Parámetros Académicos de las Instituciones de Estudios en Inteligencia Estratégica								
País	Centro Educativo Civil	Acreditado	Post grado	Acceso abierto#	Centro Educativo Militar	Acreditado	Post grado	Acceso abierto##
Argentina	ENI	X	X	X	IIFA	X	X	X
Bolivia					ECEME		X	X
Brasil	ESINT			X	ESG		X	X
Chile	UChile(*)(**)	X	X	X	ANEPE		X	X
Colombia	Incierto(**)				ESICI	X	X	X
Ecuador					(**)			
Estados Unidos	Universidades varias	X	X	X	NIU	X	X	
Guatemala	INEES(**)				CD y CESN			
México	ESISEN		X				X	
Paraguay							X	X
Perú	ENI		X	X	CAEN		X	X
Uruguay					IMES		X	X
Venezuela	CEI(**)				UMBV			

(\*) A través de la Academia de Guerra del Ejército.

(\*\*) Programa incierto o discontinuado.

# Para las instituciones civiles, el estado “abierto” significa que hay participación para funcionarios de todo el gobierno y para profesionales civiles.

## Para las instituciones militares, el estado “abierto” significa que hay participación de militares extranjeros. Son excepciones el caso de Perú, donde el CAEN sirve a personal civil del gobierno y está abierto a la sociedad, y el caso de Uruguay donde el IMES sirve a personal civil del gobierno.

Russell G. Swenson y Carolina Sancho Hirane

Anexo 2 (Tabla 17)				
Hoja de Evaluación Curricular (Ejemplo)				
Apellidos y nombres: .....				
CLASIFICACION				
Cargo Funcional: .....				
Área en que trabaja:..... Fecha de Ingreso.....				
Nivel Educativo	Tipo de titulación o actividad académica	Escala	Cantidad de actividades	Puntaje final
Postgrado	Maestría	100 pts		
Postgrado	Maestría	80 pts		
Postgrado	Especialización	60 pts		
Grado	Titulación universitaria mayor a cuatro años	50 pts		
Grado	Titulación universitaria menor a cuatro años	40 pts		
Técnico	Técnico Superior	30 pts		
Capacitación	Diplomas, Certificados y Constancias por actividades mayores a un año	30 pts		
Capacitación	Diplomas, Certificados y Constancias por actividades menores a un año hasta seis meses	20 pts		
Capacitación	Diplomas, Certificados y Constancias por actividades menores a seis meses	10 pts		
Puntaje total				
OBSERVACIONES:				
-----				
-----				
Realizado por: _____ Fecha: _____				
(La información incluida en esta hoja es meramente ilustrativa a efectos de orientar en el ejemplo presentado)				

## Gestión de Inteligencia en las Américas

Anexo 3 (Tabla 18)	
Hoja de Evaluación del Desempeño Laboral (Ejemplo)	
<b>TOTAL DE PUNTAJE OBTENIDO</b>	<b>GRADOS DE CALIFICACION</b> (Seleccione el grado que refleja la calificación de acuerdo al instructivo)
	A excelente B bueno C aceptable D regular E insatisfactorio

FACTORES DE VALORIZACION	Insatisfactorio	Regular	Aceptable	Bueno	Excelente
FACTORES INSTITUCIONALES					
<b>DOMINIO DE LA FUNCION</b> Considera dominio y familiarización del evaluado con las actividades del cargo que desempeña.	8 No posee conocimientos ni habilidades para el desempeño del cargo.	16 Conoce sus obligaciones sin llegar al dominio.	24 Conoce sus obligaciones satisfactoriamente.	32 Conoce bien sus obligaciones y cada día se supera en el mejor desempeño de sus labores.	40 Conoce perfectamente sus obligaciones y demuestra condiciones excepcionales para su trabajo.
<b>CUMPLIMIENTO DE LAS NORMAS</b> Considera el dominio y la familiarización del evaluado con las normas que regulan su actividad.	8 No ajusta a las normas y carece de conocimiento de las mismas.	12 El cumplimiento de las normas es limitado.	10 Da cumplimiento a las normas satisfactoriamente.	14 Da cumplimiento a las normas y tiene comprensión.	18 Excelente cumplimiento y gran comprensión de las normas.
<b>RESPONSABILIDAD</b> Considera la actualización del evaluado para solucionar en forma oportuna situaciones difíciles.	8 Requiere supervisión permanente por sus continuos errores.	12 Necesita Frecuentemente supervisión.	20 Requiere eventual supervisión.	28 Requiere supervisión en casos especiales.	30 No requiere supervisión.



Anexo 3 (Tabla 18), (continua)  
 Hoja de Evaluación del Desempeño Laboral (Ejemplo)

FACTORES INDIVIDUALES					
<b>CONOCIMIENTO</b> Considera el conocimiento académico del evaluado en relación a su trabajo.	8 No posee conocimiento académico	16 Posee limitado conocimiento académico. No lo aplica a su trabajo.	24 Posee conocimiento académico que aplica con limitaciones a su trabajo.	32 Posee conocimiento académico suficiente que aplica a su trabajo.	40 Posee sobresaliente conocimiento académico que aplica a su trabajo.
<b>CAPACIDAD DE ASESORAMIENTO DE INFORMACION</b> Considera la habilidad para transmitir conocimientos, ideas y sugerencias.	8 Dificultades para analizar las cuestiones a su cargo y sacar conclusiones.	16 Suele tener dificultades en el análisis y al relacionar ideas.	24 Analiza integralmente las cuestiones sometidas a su estudio.	32 Analiza satisfactoriamente las situaciones en su trabajo específico.	40 Sobresaliente analítica en el ejercicio de su especialidad. Analiza y evalúa con sobresaliente precisión.
<b>ANALISIS</b> Considera la aplicación de sus capacidades intelectuales para el análisis sistemático de información.	8 Carece de capacidad de análisis.	12 Muestra limitaciones en desarrollo de análisis.	24 Desarrolla análisis en forma aceptable.	32 Posee una elevada capacidad de análisis.	40 Su capacidad de análisis es sobresaliente.
FACTORES DE RENDIMIENTO					
<b>GRADO DE CUMPLIMIENTO DE LAS TAREAS</b> Considera el empeño del evaluado para cumplir con sus deberes	8 Es lento en sus labores y generalmente las incumple.	16 Cumple con sus labores para salir del paso.	24 Cumple sus labores en forma aceptable.	32 Pone empeño para cumplir con sus labores.	38 Es muy cumplidor en sus labores.
<b>CALIDAD DE TRABAJO REALIZADO</b> Considera la aplicación del conocimiento, experiencia y minuciosidad que el evaluado pone en su trabajo.	8 Comete errores con frecuencia y su trabajo es insatisfactorio.	16 Cumple con limitaciones su trabajo, debe mejorar la calidad.	24 Cumple su trabajo en forma aceptable.	32 Hace su trabajo con exactitud, pulcritud y minuciosidad.	40 Su trabajo es excepcional, de alta calidad y se supera cada vez más.

## Gestión de Inteligencia en las Américas

Anexo 3 (Tabla 18), (continua) Hoja de Evaluación del Desempeño Laboral (Ejemplo)					
<b>CANTIDAD DE TRABAJO REALIZADO</b> Considera el volumen de trabajo que habitualmente puede desarrollar el evaluado.	4 Su trabajo es escaso.	8 Tiene limitaciones en cuanto a su cantidad.	16 La cantidad es aceptable.	20 Pone empeño para realizar la mayor cantidad de trabajo.	24 Se esfuerza por producir cada vez mayor cantidad de trabajo.
OBSERVACIONES: ----- ----- -----					
Realizado por: _____ Fecha: _____ (La información incluida en esta hoja es meramente ilustrativa a efectos de orientar en el ejemplo presentado).					

Anexo 4 (Tabla 19)  
Instrucciones de Entrevistar

*Uso de la guía de la entrevista*

Para prepararse para la entrevista, repase los formularios de especificaciones de personal, desarrolle un juego de preguntas generales y específicas a ser tratadas durante la entrevista, en la guía de entrevista establezca el número de preguntas a formular y anote preguntas adicionales pertinentes. Proceda basándose en la guía de la entrevista, empleando las preguntas de introducción para cada área y otras preguntas selectas. Mezcle preguntas y aseveraciones y use frases de introducción para quitar la apariencia de interrogatorio. Las preguntas se presentan en forma condensada para ahorrar espacio.

*Uso de la sección de evaluación del candidato*

Evalúe al candidato con respecto a los factores principales de acuerdo a su opinión. Finalizada la entrevista, convierta sus notas en una evaluación. Al hacer la evaluación final debe determinar la importancia de cada factor con respecto a las exigencias laborales. Debe documentar sus impresiones y los puntos más relevantes de la información obtenida en los espacios establecidos para “comentarios”, “cualidades notables”, “puntos débiles” y “resumen total”. Preste especial atención a las cualidades notables y los puntos débiles que se relacionen con los requisitos críticos del trabajo. Luego, transfiera su evaluación del candidato con respecto a cada factor a la tabla de resumen de evaluación.

**GUÍA DE LA ENTREVISTA**

1. Comience relatándome su experiencia de trabajo en la organización de inteligencia, desde su primer trabajo hasta su puesto actual. Por cada trabajo quiero saber lo que hacía, lo que agradaba, lo que desagradaba, su sueldo y cualquier logro especial.
2. ¿Qué nivel de estudios y que capacitaciones académicas posee? ¿Le han servido sus estudios para aplicarlos a su trabajo?
3. ¿Qué conocimientos de sus estudios académicos cree que le han sido de mayor utilidad para su trabajo? ¿Cuáles cree que deben ser los conocimientos que deberían enfatizarse para que sean más útiles a su profesión?

### Anexo 4 (Tabla 19), (continua) Instrucciones de Entrevistar

4. ¿Puede darme uno o dos ejemplos en los que sus conocimientos académicos le han sido de utilidad en su trabajo?
5. ¿Sus conocimientos académicos hacen su trabajo más eficaz que otros que trabajan con usted y que no poseen similares estudios?
6. ¿Cree que la organización a la que pertenece valora los títulos académicos que posee? ¿Ha notado un mayor crecimiento profesional por tener títulos académicos, tales como ascensos, reconocimientos, mayor salario?
7. ¿Cree que existe una correlación entre los grados académicos obtenidos con una mayor relación con funcionarios del gobierno, académicos y miembros de organizaciones similares de otros países?

Anexo 4 (Tabla 19), (continua)  
Instrucciones de Entrevistar

Hoja de Entrevista Personal (Ejemplo)

**I. DATOS GENERALES :**

**CLASIFICACION**

Nombres y Apellidos: .....

Cargo Funcional: .....

Fecha de ingreso: .....

**II. ENTREVISTA PERSONAL**

**CRITERIOS:**

Presentación hasta 10 puntos : ( )  
(Mide actitudes y personalidad)

Seguridad y Convencimiento, hasta 20 puntos : ( )  
(Mide Comprensión y Habilidad)

Razonabilidad, hasta 10 puntos : ( )  
(Mide Capacidad de Análisis)

Adaptabilidad, hasta 10 puntos : ( )  
(Mide Ubicación en su Trabajo)

Conocimientos, hasta 20 puntos : ( )  
(Mide Conocimientos específicos- Relación Institucional)

**III. CONSIDERACIONES DEL EVALUADOR**

Comentarios:

.....

Cualidades  
notables:

.....

Puntos débiles:

.....

Resumen total:

.....

Puntaje:.....

## Gestión de Inteligencia en las Américas

Anexo 4 (Tabla 19), (continua)	
Instrucciones de Entrevistar	
<b>GRADOS DE CALIFICACION</b> (Seleccione el grado que refleja la calificación)	
A excelente B bueno C aceptable D regular E insatisfactorio	
Realizado por: _____ Fecha: _____	
Firma del evaluado:..... (La información incluida en esta hoja es meramente ilustrativa a efectos de orientar en el ejemplo presentado)	

Anexo 5 (Tabla 20) Hoja de Evaluación de Conocimientos (Ejemplo)	
Apellidos y nombres: .....	
CLASIFICACION	
Cargo Funcional: .....	
Fecha de Ingreso.....	

	Responda las siguientes preguntas:	Puntaje
1	La Inteligencia Estratégica es una ciencia o un arte? Fundamente su opinión.	
2	Qué herramientas tecnológicas para la gestión del conocimiento conoce? Describalas.	
3	Cuál es el concepto de Seguridad Nacional vigente?	
4	Cuáles son los presupuestos éticos de la profesión? Proporcione ejemplos.	
5	Describa el significado de la “sorpresa estratégica” de carácter diplomático.	
6	Cómo se relaciona la cultura nacional del país con la inteligencia estratégica nacional?	
7	De acuerdo a las normas legales vigentes, cuáles son las características, atribuciones y limitaciones de la organización a la que pertenece?	
8	Qué tareas cumple el Cuarto Departamento del Estado Mayor del Ejército Popular de Liberación de China?	
9	Qué relación tiene la Inteligencia Estratégica con las oportunidades estratégicas?	
10	El principio dialógico, el principio recursivo y el principio hologramático, conforman los tres principios básicos de un método de pensamiento. Identifique y describa el método de que se trata.	
	Puntaje total	

## Gestión de Inteligencia en las Américas

Anexo 5 (Tabla 20), (continua)	
Hoja de Evaluación de Conocimientos (Ejemplo)	
GRADOS DE CALIFICACION (Seleccione el grado que refleja la calificación)	
A excelente B bueno C aceptable D regular E insatisfactorio	
OBSERVACIONES: ----- ----- -----	
Realizado por: _____ Fecha: _____ (La información incluida en esta hoja es meramente ilustrativa a efectos de orientar en el ejemplo presentado)	



Anexo 6 (Tabla 21) Hoja de Resumen de Evaluación Individual (Ejemplo)	
<b>DATOS GENERALES:</b> <span style="float: right;"><b>CLASIFICACION</b></span> Nombres y Apellidos: ..... Cargo Funcional: ..... Fecha de ingreso: .....	
<b>I. EVALUACION CURRICULAR</b> PUNTAJE OBTENIDO: .....	
<b>II. DESEMPEÑO LABORAL</b> PUNTAJE OBTENIDO: .....	
<b>III. ENTREVISTA PERSONAL</b> PUNTAJE OBTENIDO: .....	
<b>IV. EVALUACION DE CONOCIMIENTOS</b> PUNTAJE OBTENIDO: .....	
<b>FACTOR</b>	<b>VALOR</b>
1	
2	
3	
4	
Subtotal	
<b>PUNTAJE FINAL OBTENIDO EN EL PROCESO DE                      EVALUACION INDIVIDUAL: .....</b>	
<b>GRADOS DE CALIFICACION</b> (Seleccione el grado que refleja la calificación según instructivo)	
A excelente B bueno	
C aceptable D regular E insatisfactorio	

## Gestión de Inteligencia en las Américas

Anexo 6 (Tabla 21) Hoja de Resumen de Evaluación Individual (Ejemplo)
OBSERVACIONES:  -----  -----  Realizado por: _____ Fecha: _____ (La información incluida en esta hoja es meramente ilustrativa a efectos de orientar en el ejemplo presentado)

**Fuente:** Tablas/anexos creados por el autor.



## Manejo y Gestión de la Información de Inteligencia para la Seguridad Multilateral del Ciberespacio- Enfoques de los Estados Unidos y Brasil

Robin M. Rogers

*La complicación política y legal en lo virtual es mucho más difícil de lo que es en otros ámbitos.*

-William Lynn III<sup>689</sup>

### Preparando el escenario

Diariamente, informes de prensa afirman que algún gobierno, compañía o grupo de ciudadanos han sido “atacados” a través del ciberespacio. Con frecuencia, estos informes son exagerados, incluyendo palabras que pueden provocar una respuesta desproporcionada a los actuales eventos. Esto no quiere decir que el ciberespacio no sea un lugar peligroso. Mucha gente activa en el ciberespacio representa una amenaza para la seguridad nacional, seguridad económica e inclusive para la seguridad personal. Algunas de estas personas actúan por su cuenta; algunos como parte de una banda criminal o grupos de activistas políticos; y algunos actúan como agentes para potencias extranjeras — ya sea para cometer espionaje o para llevar a cabo lo que muchos definirían como “operaciones militares”.

Los responsables de inteligencia pueden tomar ventaja de un esfuerzo coordinado entre las comunidades del sector privado, orden público, militar e inteligencia para defender el ciberespacio. El ingrediente esencial de esta coordinación es el intercambio de información — ya sea información de dominio privado, información de orden público o de inteligencia. Los obstáculos para el intercambio de la información incluyen no sólo incertidumbre acerca de qué compartir, sino también qué podría o qué debería ser intercambiado. Estos obstáculos son combinados cuando los países necesitan intercambiar información de inteligencia entre sí.

Desde la perspectiva de un responsable de inteligencia, este ensayo estudia y refuerza la importancia del intercambio de información, primero al tratar el tema de la terminología común e inclusive el lenguaje, luego al tratar

la amenaza que los actores en el ciberespacio representan para la seguridad nacional, económica y personal. Las acciones que Estados Unidos y Brasil están tomando para responder a la amenaza cibernética ilustran los desafíos para manejar de manera inteligente la información de inteligencia y el ensayo concluye con la exploración de posibles mejoras en las políticas y prácticas del manejo de la información de seguridad cibernética.

### Necesidad de aceptar la amenaza del ciberespacio

Uno de los problemas más desconcertantes para los responsables de inteligencia es cómo describir la amenaza especificada, en la que los responsables de inteligencia usan términos de diferentes ámbitos del mundo de los especialistas militares, de inteligencia, y del orden público. Además, varias culturas del sector privado (incluyendo la industria de internet), de medios de comunicación masiva, e inclusive de la seguridad cibernética utilizan diferentes términos para la misma cosa — ya sea para describir un evento ordinario o una amenaza inminente. De igual manera, en ocasiones, los representantes de estos sectores usan un mismo término que tiene diferentes significados.

Un punto lógico para comenzar es ofrecer una propia definición del ciberespacio. En los Estados Unidos hay varias definiciones. La *Cyberspace Policy Review* lo define como la “infraestructura de comunicación e información digital interconectada globalmente”.<sup>690</sup> Esa misma apreciación define al ciberespacio más detalladamente como “la red interdependiente de infraestructuras de tecnología de información, e incluye internet, redes de telecomunicación, sistemas informáticos, y procesadores y controles insertados en industrias críticas”.<sup>691</sup> Un sitio de Tecnología de Información (IT) lo define como una “metáfora para describir el terreno no físico creado por sistemas informáticos”.<sup>692</sup> Otro concepto surge en la República Checa, con el uso de términos igualmente generales: “El ciberespacio es actualmente utilizado para describir el ámbito total de recursos de información disponibles a través de redes informáticas”.<sup>693</sup>

Eludiendo otras caracterizaciones del ciberespacio, este ensayo emplea una definición más precisa: “El ciberespacio es un dominio operacional cuyo carácter único y distintivo está rodeado por el uso de aparatos electrónicos y el espectro electromagnético para crear, guardar, modificar, compartir y explotar información vía sistemas basados en tecnología de comunicación

## Gestión de Inteligencia en las Américas

de información interconectada (ICT) y sus infraestructuras relacionadas”.<sup>694</sup> Puede parecer que se necesiten muchas palabras para describir a una entidad “virtual”. Una razón para emplear esta definición, sin embargo, es que se la puede aplicar a muchas de las culturas mencionadas anteriormente. Se aplica a “objetos electrónicos” y “sistemas” e “infraestructuras”, y abarca la manera en que las personas “explotan” aquellas cosas para crear y utilizar información. La definición se detiene antes de incluir información por sí misma como parte del ciberespacio.<sup>695</sup>

Definir el ciberespacio ayuda a entender lo que sucede ahí. Este ensayo se concentra en dos de las cosas negativas que ocurren dentro de ese espacio: ataque e intrusión. Parafraseando una fuente en línea, “un ataque ciberespacial es una explotación deliberada de sistemas de computadoras, compañías dependientes de la tecnología y redes. Los ataques ciberespaciales usan códigos maliciosos para alterar la configuración del manejo lógico de la computadora, que pueden resultar en datos comprometidos o crímenes ciberespaciales, tales como el robo de información o de identidad”.<sup>696</sup> Mientras que esta definición puede servirle a las comunidades mencionadas anteriormente, no se ajusta bien a las comunidades militares o de inteligencia. La razón es que un “ataque” de cualquier tipo puede resultar en una acción militar, incluyendo una guerra. Cualquier definición sobre un ataque ciberespacial debe ser más preciso. En este ensayo, entonces, un “ataque ciberespacial” es el uso del ciberespacio para interrumpir, negar, degradar, destruir o manipular la información que reside en computadoras y redes informáticas, o las computadoras y redes mismas.<sup>697</sup>

La Oficina Federal de Investigación de Estados Unidos (FBI), usa un concepto más comprensivo que “ataque”- ellos prefieren el término “intrusión cibernética.”<sup>698</sup> Mientras que el FBI no proporciona una definición estándar, por alcance, la intrusión cibernética puede ser definida como el “acceso a una computadora (o red o sistema) sin autorización o exceder acceso autorizado, y obtener información mediante esta conducta.”<sup>699</sup> El enfoque aquí es cómo obtener acceso no autorizado. Mientras que el Instituto Nacional de Normas y Tecnología de Estados Unidos (NIST) no se refiere específicamente a “intrusión cibernética”, sí se refiere a “intrusión de red” y también usa ese término para referirse al acceso a redes no autorizado.<sup>700</sup>

En algunos casos, computadoras privadas, redes, o sistemas<sup>701</sup> pueden comunicar o contener información clasificada de seguridad nacional. En ciertos

casos, la información privada puede estar protegida con las leyes de propiedad intelectual. Y en otros casos, la información privada puede relacionarse con cuentas personales, emails y fotografías.

En los últimos dos casos, la intrusión cibernética puede ser vista claramente como un crimen ciberespacial. En el primer caso (robo de información clasificada u otra información de seguridad nacional) la acción debería ser considerada como espionaje ciberespacial. El espionaje es un crimen también; la diferencia entre el espionaje y el crimen ciberespacial generalmente determina cuales órganos del gobierno son responsables de la protección en contra del acto o de procesar a aquellos que cometieron el crimen. Las organizaciones de contrainteligencia, que pueden ser parte de las comunidades de orden público, militares o de inteligencia (en cualquier combinación) están generalmente interesadas en el espionaje ciberespacial.

Cuando se piensa acerca de información de inteligencia que apoya los esfuerzos nacionales para defenderse de cualquier amenaza de operación hostil en el ciberespacio, ya sea un ataque o intrusión, el entender quién es responsable de la defensa es importante. Las organizaciones de inteligencia necesitan familiarizarse con las necesidades de información de la organización que apoyan. La necesidad de colaborar simultáneamente con organizaciones de contrainteligencia y orden público introduce culturas adicionales, y por lo tanto demandas adicionales de información, a los responsables de inteligencia.

La idea de “atribución” es un interés similar para cualquier responsable de inteligencia con el deber de apoyar los esfuerzos de seguridad cibernética. La atribución determina “la identidad o ubicación de un atacante o un intermediario del atacante.”<sup>702</sup> La identidad podría incluir información de identificación, tal como el nombre, número de cédula, información de cuenta o alias. La ubicación puede ser virtual o física y puede incluir a los intermediarios — aquellas entidades mediante las cuales un atacante (o intruso) pasa del camino al objetivo. Los intermediarios pueden ser voluntarios o involuntarios, y a la determinación de su alianza se suma la tarea de establecer su atribución.

La variedad de fuentes citadas para las pocas definiciones mencionadas anteriormente le recuerda al responsable de inteligencia de las muchas culturas con un interés en defender el ciberespacio. El desafío es asegurar que la información intercambiada entre varias culturas sea entendida por el receptor al igual que por el transmisor. Un responsable de inteligencia tendría en cuenta

## Gestión de Inteligencia en las Américas

que las diferencias del idioma (Portugués/Inglés) y cultura (Brasil/Estados Unidos) son importantes al compartir información. Una comprensión en común de los conceptos utilizados para caracterizar amenazas de operaciones hostiles del ciberespacio también demanda nuestra atención.

### Amenazas del ciberespacio: necesidad de reconocer conceptos

Muy a menudo, una amenaza en el ciberespacio se iguala con un *efecto* creado allí. Para evitar esta confusión, los responsables de inteligencia, como en otras comunidades cibernéticas, pueden desagregar el concepto con una fórmula estándar para determinar la amenaza: intención + capacidad = amenaza. Según esta fórmula, cualquiera con la capacidad para provocar un efecto negativo también debe tener la intención de utilizar esa capacidad para ser una posible amenaza.

El Cañón de Ion de Baja Órbita (LOIC) ilustra cómo una herramienta puede permitir al actor cambiar de ser una amenaza posible a una real. Utilizada para propósitos legales, el LOIC es una herramienta que evalúa cómo una red puede soportar cargas pesadas de actividad. Utilizada como un arma de ataque ciberespacial, puede sobrecargar las redes al punto de hacerlas colapsar — creando así denegación de servicio. El LOIC es gratis y un video de *YouTube* le muestra al espectador como utilizarlo.<sup>703</sup> Esto significa que virtualmente cada persona que usa internet puede obtener la capacidad para llevar a cabo un ataque o intrusión cibernética. La capacidad no es un factor limitante.

En el ciberespacio, la intención requiere de una comprensión matizada. Una capacidad de *botnet*<sup>704</sup> permite a la persona controlar remotamente muchas otras computadoras (o inclusive redes). Obtener el control de las computadoras es generalmente una intrusión cibernética, a menos que los dueños de las computadoras controladas hayan consentido ser controlados. De cualquier manera, la *botnet* resultante es una capacidad. La persona controlándola podría querer provocar un ataque distribuido de denegación de servicios. O la intención simplemente puede ser el utilizar la *botnet* para facilitar el acceso no autorizado a otras computadoras, información o redes. En el primer caso, el efecto es un ataque ciberespacial. En el segundo caso, el efecto es una intrusión cibernética. Una intrusión cibernética pudo haber ocurrido cuando la *botnet* fue simplemente creada. La amenaza en ambos casos es el actor, no el efecto.



De acuerdo a ese modelo, los responsables de inteligencia pueden proporcionar u obtener información sobre tres categorías de amenazas. La primera es el actor estatal; la segunda el actor no estatal; y la tercera un actor solitario. Como ha demostrado la experiencia, estas categorías no son exclusivas — un actor que pertenece a una puede pertenecer a más de una. La lealtad de un actor complica la decisión de un responsable de inteligencia para compartir información sobre las amenazas en el ciberespacio: una vez que establece la atribución personal, ¿es posible hacer una conexión con un conjunto de actores más grande?

Durante muchos años, las compañías privadas de seguridad cibernética, junto con organizaciones gubernamentales que lidian con la tecnología de la información, policiales e inteligencia pusieron al actor Estado-Nación al tope de las amenazas cibernéticas. De muchas maneras, todavía lo es. El Equipo de Preparación Informática de Emergencia de EE.UU., (US-CERT), declara que los programas de Estado-Nación

son únicos al representar una amenaza a lo largo del espectro total de objetivos que podrían perjudicar los intereses de los Estados Unidos. Estas amenazas varían desde propagandas a alteraciones menores de sitios Web a espionaje y serias perturbaciones, con la pérdida de vidas y interrupción prolongada de los servicios prestados por la infraestructura. Entre la matriz de amenazas cibernéticas, como se ve hoy en día, sólo los programas patrocinados por el gobierno están desarrollando capacidades con el prospecto futuro de provocar daño generalizado de larga duración.<sup>705</sup>

Inclusive con las advertencias del pasado, ahora no vigentes, indican que más de 120 países cuentan con o se encuentran desarrollando capacidades de ataque o intrusión ciberespacial.<sup>706</sup>

Se asume que no todos los actores de Estado-Nación tienen capacidades sofisticadas. Algunas Estados-Nación no democráticas pueden de hecho emplear sus capacidades contra lo que ellos perciben como amenazas internas, por lo tanto su intención es clave para determinar la amenaza.

Algunos actores estatales parecen tener mayor interés en las intrusiones cibernéticas, con el objetivo de obtener información de seguridad nacional. Así, el

## Gestión de Inteligencia en las Américas

Secretario de Defensa de EE.UU. Leon Panetta, en 2012 confirmó que China es responsable de obtener información clasificada de computadoras y sistemas del Departamento de Defensa de Estados Unidos.<sup>707</sup>

Los actores no estatales aparecen en muchas formas. Los criminales ciberespaciales son quizás la primera variedad que resalta, y están generalmente motivados por la codicia. La amenaza por parte de la mayoría de los criminales ciberespaciales no es el ataque ciberespacial -excepto en casos donde la extorsión esté involucrada- sino que éstos crean intrusiones en su mayoría para obtener datos o acceder a información de cuentas financieras. Tal actividad puede ser atribuida a individuos dentro de un país, de hecho la “organización” *Shadowcrew* condujo operaciones de intrusión en una escala global desde el año 2002 al 2004, robando información de crédito o identidades de individuos de numerosos Estados.<sup>708</sup> Una publicación reciente de *Pricewaterhouse Coopers Brazil Ltda* indica que el crimen ciberespacial era la segunda actividad criminal en Brasil en el año 2011.<sup>709</sup> La compañía de seguridad de internet *Norton*, en su reporte de crimen ciberespacial para el año 2011, declara que el costo total neto del crimen ciberespacial en los Estados Unidos para el año 2011 fue de \$139,6 billones, mientras que la pérdida neta a nivel mundial fue de \$388 billones.<sup>710</sup>

La mayoría del crimen ciberespacial en países líderes es llevado a cabo en contra del sector privado, lo cual incluye a personas físicas. Las intrusiones cibernéticas contra objetivos de seguridad nacional (información clasificada, información guardada por gobiernos o por contratistas del gobierno) no son usualmente conducidas por criminales ciberespaciales, pero a veces sí por actores no estatales tales como los *hackers* patrióticos que delinquen desde China o grupos activistas de *hackers* tales como *Anonymous* o *Lulzsec*.

Como ejemplo de actores no estatales que llevan a cabo intrusiones cibernéticas tenemos la “confrontación” entre *hackers* chinos patrióticos y aquellos de las Filipinas sobre derechos de pesca en el *Scarborough Shoal*, (o, como los chinos se refieren a ella, Isla Huangyan). Los *hackers* chinos patrióticos, en protesta contra el gobierno Filipino luego de que la Marina filipina intentó arrestar a algunos pescadores chinos por pescar ilegalmente en el área, interrumpieron los sitios gubernamentales filipinos. Estas acciones no fueron por intrusos del gobierno chino, sino por parte de *hackers* chinos patrióticos actuando independientemente.<sup>711</sup> Mientras que estos “*hackers* patrióticos” no

estatales están involucrados en un comportamiento criminal, generalmente no lo hacen con fines de lucro monetario.

Otro grupo no estatal que representa una amenaza hostil en el ciberespacio son los activistas hackers. Mientras que éstos han estado conduciendo intrusiones por varios años, la amenaza que representan se ha convertido en la misma que la de algunos actores estatales, aun si el motivo es diferente. La revista *Wired* ha reportado que los activistas hackers han superado a los criminales ciberespaciales en el 2011.<sup>712</sup> La compañía de seguridad cibernética *Kaspersky* colocó el incremento del “activismo *hacker*” al tope de las nuevas amenazas del 2011.<sup>713</sup> Los activistas hacker tales como los grupos *Anonymous* y *Lulzsec* están entre aquellos de mayor interés para las comunidades de orden público y de seguridad nacional.

*Anonymous* es una colección amorfa de individuos que buscan, en general, protestar por lo que ellos consideran objetable, tales como la Iglesia de la Cienciología, o los esfuerzos para detener a Wikileaks.<sup>714</sup> Sus protestas pueden ser en forma de ataques dirigidos a la denegación de servicio, donde un sitio en particular, servidor o computadora es inundado con mails o pedidos hasta el punto en que el sitio, servidor o computadora es forzado a cerrar. Otras protestas intentan alterar un sitio, muchas veces remplazando información o imágenes con declaraciones sobre sus propias habilidades. Pero otra perspectiva es llevar a cabo una intrusión cibernética que roba información, generalmente nombres, mails u otra información personal del dueño de la cuenta. La motivación es protestar — y generalmente las protestas son a una escala global. Muchas de las actividades de este grupo pueden ser consideradas como crímenes ciberespaciales mientras sean dirigidos contra organizaciones privadas. Afirma haber interrumpido sitios de varias organizaciones gubernamentales británicas,<sup>715</sup> una acción que tiende a cruzar de una actividad criminal a una amenaza a la seguridad nacional.

*Lulzsec* es un grupo de individuos (activistas hackers) mucho más pequeño que tiene metas con menor definición (o sin metas más allá de la diversión en crear caos), pero usan las mismas herramientas como *Anonymous* para expresar sus puntos de vista a través del ciberespacio. Este grupo reclama responsabilidad por varias intrusiones y ataques. Las intrusiones incluyen el robo de información administrativa y del usuario de sitios de *Sony*. La motivación, aparentemente, fue demostrar que la seguridad cibernética de *Sony*

## Gestión de Inteligencia en las Américas

no era muy buena.<sup>716</sup> *Lulzsec* también ha reclamado haber atacado, utilizando denegación de servicio (DDoS), varios sitios del gobierno brasileño,<sup>717</sup> el sitio de una organización afiliada al FBI llamada *Infraguard*,<sup>718</sup> al igual que sitios de la Agencia Central de Inteligencia de EE.UU. (CIA) accesibles al público.<sup>719</sup> Al igual que *Anonymous* en algunos casos, este grupo de activistas hackers representan un desafío tanto para las comunidades de orden público (la intrusión a *Sony* e *Infraguard*) y de seguridad nacional (los ataques contra los sitios de los gobiernos de Estados Unidos y Brasil).

Una tercera amenaza de acción hostil en el ciberespacio es el actor individual a veces llamado *hacker*. Un ejemplo de actor solitario es Kevin Mitnik, una vez descrito como uno de los criminales informáticos más buscados en los Estados Unidos.<sup>720</sup> Mitnik fue acusado de haber obtenido acceso no autorizado a un gran número de compañías y sistemas informáticos, y de robar información de tarjetas de crédito de más de 20,000 personas a nivel mundial. Mitnik declaró que su motivación en esta actividad de *hacker* fue “aprender, no causar daño”.<sup>721</sup>

Un ataque (tal como la DDoS) puede ser visto como un acto criminal, o como un acto que puede caber bajo la Ley de Conflicto Armado y así provocar una respuesta militar. Una herramienta utilizada para llevar a cabo un ataque DDoS puede ser la misma herramienta usada para denegar acceso a las cuentas bancarias de los clientes o denegar acceso a un comandante militar a sus fuerzas de despliegue. Sin embargo, la respuesta apropiada para el uso de esta herramienta debería variar dramáticamente. Las decisiones legales y de políticas (nacional e internacional) deberían ser utilizadas para determinar la respuesta. Los responsables de inteligencia, oficiales del orden público, o personas que trabajen para instituciones privadas de seguridad cibernética deberían poder proporcionar la información útil para la toma necesaria de decisión legal y de política.

Una intrusión representa un desafío similar, pero los responsables de inteligencia enfrentan aún más incertidumbre con respecto al intercambio de información sobre la intrusión. Ambos, ataques e intrusión deben comenzar con un actor de amenaza obteniendo acceso no autorizado a un sistema o red. En algunos casos las herramientas y vulnerabilidades que emplea un actor de amenaza para una intrusión sería la misma herramienta y vulnerabilidad empleada para un ataque. Determinar la intención de un amenazador se

convierte en la clave y a veces no se sabe hasta que el ataque (o intrusión) ha ocurrido. Ya que la acción misma debería determinar la respuesta, es muy difícil saber si las fuerzas de defensa de orden público y militares deberían ser responsables de la prevención o respuesta al incidente.

### Evaluación de las ciberamenazas por parte del responsable de inteligencia

Un responsable de inteligencia eficaz debe tener un conjunto de requerimientos con los cuales trabaja. Aquellos requerimientos (algunos pueden llamarlos información demandada) guiarán al responsable para saber contra quién tienen que recopilar información y de igual importancia, saber quién ha dicho que la necesita. Este último aspecto es importante por varias razones — saber quién quiere/necesita la información de inteligencia puede ayudar al responsable de inteligencia entender por qué existe esa necesidad, quién más quiere/necesita la información de inteligencia, y cómo (en qué formato) se debe entregar la información.

Los observadores de seguridad cibernética de la tecnología de información de gobierno, legisladores, académicos y del sector privado han proporcionado opiniones sobre quién es responsable dentro y fuera del gobierno de la protección contra amenazas de acción hostil en el ciberespacio. Las opiniones varían y son la causa de debates continuos. Las preguntas que marcan al debate incluyen: 1) ¿Quién es responsable de proteger la información de seguridad nacional e infraestructura crítica de la nación, y cuál es esa infraestructura?; un corolario a esta pregunta es ¿Quién establecerá las reglas de enfrentamiento para acciones ofensivas y defensivas contra oponentes ciberespaciales?; 2) ¿Quién es el responsable de proteger la infraestructura que las sociedades necesitan ahora ya que sus operaciones dependen de la seguridad del ciberespacio, y que es *aquella* infraestructura?; 3) ¿Quién es responsable de proteger la propiedad intelectual?; y 4) ¿Quién protegerá el acceso a la información privada asociada con la identidad de documentos y cuentas bancarias? Los responsables de inteligencia no deberían responder tales preguntas, pero sin embargo sí podrían beneficiarse del conocimiento de estas respuestas para así poder asegurar que pueden proporcionar el nivel apropiado de información a aquellos que son responsables.

## Gestión de Inteligencia en las Américas

El presente ensayo no puede responder a todas esas preguntas, pero como una disciplina que conjuga la recolección de información proactiva, el manejo de información, el análisis como eje de la actividad, y la responsabilidad de desarrollar estrategias de evaluación para los líderes nacionales, la función de inteligencia y sus responsables están en posiciones favorables para proporcionar una comprensión inicial o evaluación neta del conflicto ciberespacial. Además, debido a que la Comunidad de Inteligencia de Estados Unidos tiene un fuerte programa para evaluar amenazas y oportunidades tanto externas como internas, y la comprensión propia de lo familiar es a veces mejorada por la referencia a algo menos familiar, pero que presenta un conjunto similar de circunstancias, este ensayo examinará el estado de los ajustes a la seguridad cibernética de Brasil como un referente para mejorar nuestra comprensión de la situación de Estados Unidos.

En el 2001, el Congreso de Estados Unidos reconoció esto cuando promulgó una ley por la cual los “negocios privados, gobierno, y el aparato de seguridad nacional depende cada vez más de una red interdependiente de infraestructuras críticas de información y físicas, incluyendo telecomunicaciones, energía, servicios financieros, agua, y sectores de transportación.”<sup>722</sup> Esa red interdependiente es el espacio cibernético. El Banco Mundial reporta que en el año 2010, 75% de las personas en los Estados Unidos, y un poco más del 40% de la población de Brasil, estaban activos en el espacio cibernético.<sup>723</sup>

Muchos gobiernos de la región arriendan las líneas de comunicación comerciales, e inclusive los aparatos comerciales. Las Fuerzas Armadas de Estados Unidos dependen de algunas líneas de comunicación alquiladas<sup>724</sup> y esas líneas son parte del dominio cibernético. Así la información crítica militar y de infraestructura puede estar o pasar a través del mismo espacio cibernético como la información de propiedad intelectual de una compañía privada, o la información bancaria de un ciudadano privado. En los Estados Unidos, el personal y agencias responsables de proteger la infraestructura cibernética incluyen al Departamento de Defensa, Seguridad Nacional, Justicia y Comercio, al igual que la Comunidad de Inteligencia en general.<sup>725</sup>

Siete Centros de Seguridad Nacional Cibernética de los Estados Unidos apoyan a las comunidades de inteligencia, defensa, civil, orden público/contrainteligencia en el Gobierno de los Estados Unidos. Al menos tres de ellos también proporcionan apoyo y guía a usuarios no gubernamentales.<sup>726</sup>

La figura 13 muestra los centros, comunidades a las cuales pertenecen principalmente, y qué autoridades/responsabilidades tienen. También se enumeran las funciones las que cada uno supuestamente debe dedicarse.

Nótese que estos centros no incluyen de forma directa ninguna empresa comercial u organización académica. Sin embargo, U.S. CERT y el NCCIC (mediante centros regionales y temáticos para compartir y analizar información (ISACs)), sí ofrecen datos a la industria del internet y a otras entidades privadas. Además, el NCIJTF da apoyo a otras agencias reguladoras y de las fuerzas del orden. Cualquier centro puede ofrecer información de utilidad a otros. Pero el NCCIC es responsable de tal coordinación. En cuanto a los aspectos internacionales de la ciberseguridad, los representantes del Departamento del Estado estadounidense juegan un rol directamente en algunos de los centros, para supervisar acciones relacionadas con el exterior.

Un responsable de inteligencia que responde a demandas de información similares para el gobierno de Brasil también enfrenta un desafío complejo. Tal como en los Estados Unidos, muchas organizaciones están involucradas en proveer seguridad cibernética para el gobierno y la sociedad. La figura 14 muestra a algunas de estas organizaciones, sus funciones y sus responsabilidades. CERT.br, el Equipo de Respuesta a Emergencia Informática de Brasil, funciona de manera parecida al US-CERT.<sup>727</sup> SERPRO es una compañía pública/privada que proporciona procesamiento de información para muchos sectores civiles del Gobierno Federal de Brasil.<sup>728</sup>

La Policía Federal de Brasil es la organización policial primaria para la seguridad cibernética,<sup>729</sup> aunque la policía de los diferentes estados que componen la República Federativa de Brasil también es responsable de la aplicación de la ley en el espacio cibernético.<sup>730</sup> La Oficina del Fiscal Federal de Brasil y el Ministerio de Justicia también están involucrados en la gestión del proceso judicial contra actividades cibernéticas criminales. Estas dos tienen responsabilidades similares a las del FBI de EE.UU. El Centro de Defensa Cibernética de Brasil (CDCIBER) es la organización federal encargada de proteger la red militar y gubernamental, al igual que la información de infraestructura de Brasil en conjunto.<sup>731</sup> Al Ejército de Brasil se le ha dado la ventaja de crear y manejar esta organización, que tiene responsabilidades similares a las del Comando Cibernético de Estados Unidos. El GSI de Brasil (Gabinete de Seguridad Institucional) desempeña una función paralela a la de la Comunidad de

### Centros de Ciberseguridad Federal de los Estados Unidos

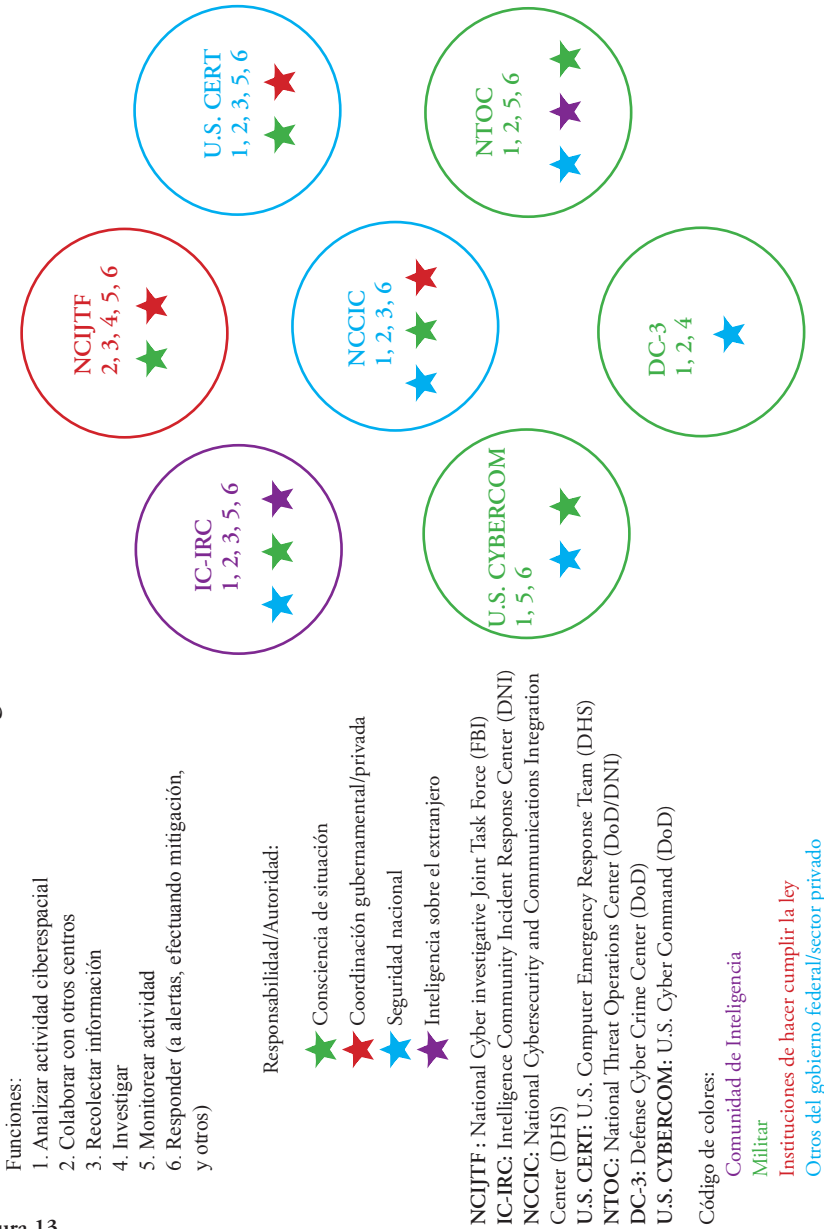


Figura 13.

Fuente: Desarrollada por el autor. Datos del 2012.







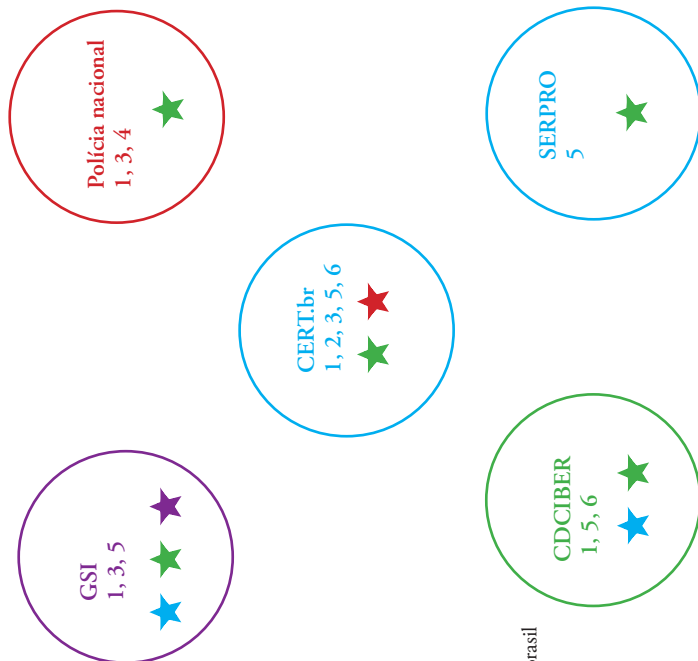
## Instituciones Brasileñas de Ciberseguridad Gubernamental

### Funciones:

1. Análisis de actividad ciberespacial
2. Efectuando colaboración con otros centros
3. Recolección de información
4. Investigación
5. Monitoreo de actividad
6. Respondiendo (a alertas, efectuando mitigación, y otros)

### Responsabilidad/Autoridad:

-  Consciencia situacional
-  Coordinación gubernamental/privada
-  Seguridad nacional
-  Inteligencia sobre el extranjero



GSI: Gabinete de Segurança Institucional - Inteligência  
 CERT.br: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança, por parte del CGI.br: Comitê Gestor de Internet en Brasil  
 CDCIBER: Centro de Defesa Cibernética (MoD)  
 Polícia nacional: Ministério de Justiça  
 SERPRO: Serviço Federal de Processamento de Dados

### Código de colores:

- Comunidade de Inteligência
- Militar
- Instituições de hacer cumplir la ley
- Otros del gobierno federal/sector privado

Figura 14.

Fuente: Desarrollada por el autor. Datos del 2012.

## Gestión de Inteligencia en las Américas

Inteligencia de Estados Unidos. La Agencia de Inteligencia de Brasil (ABIN), una organización civil, está dentro del GSI.<sup>732</sup> Finalmente, el Departamento de Seguridad de Información y Comunicación (DSIC) proporciona seguridad cibernética para el Poder Ejecutivo del Gobierno de Brasil.<sup>733</sup>

Entre las ilustraciones de los esfuerzos de seguridad cibernética de Estados Unidos y Brasil destacan los intereses superpuestos de varias organizaciones responsables de tratar acciones hostiles del ciberespacio. Mientras que algunas estructuras son paralelas, hay una diferencia muy obvia representada en las líneas de comunicación/intercambio de información. Las líneas son virtualmente inexistentes para Brasil, mientras que el número de líneas entre los centros de Estados Unidos pueden generar tanto intercambio de información que la detección de reportes repetitivos y circulantes puede convertirse en un problema.

En entrevistas, el General José Carlos dos Santos, comandante del CDCiber, indicó que se encontraba trabajando para establecer relaciones cercanas con el GSI, al igual que SERPRO.<sup>734</sup> Sin embargo, tales esfuerzos aparentemente no son aplicados a lo largo de la comunidad. Un policía civil experto en asuntos del espacio virtual, Emerson Wendt, comentó que el Comité Directivo de Internet de Brasil (CGI.br) simplemente recibe información, y no la intercambia con otras organizaciones con responsabilidades de seguridad cibernética.<sup>735</sup> CERT.br, una organización subordinada a CGI.br, es responsable de los reportes de incidentes de seguridad informática en Brasil cuyo papel y autoridad en proporcionar advertencias no es claro aún.<sup>736</sup>

Así como un responsable de inteligencia apoya los esfuerzos de Estados Unidos para defender al espacio cibernético, un responsable de inteligencia de Brasil tiene la oportunidad de anticipar y advertir las amenazas cibernéticas, teniendo en cuenta los distintos arreglos institucionales del país, establecidos para gestionar varios aspectos de ataques cibernéticos actuales y futuros, junto con las intrusiones. Al parecer, un responsable de inteligencia de Brasil enfrenta un servicio de intercambio de información menos complejo que el de los Estados Unidos.

### Seguridad del ciberespacio desde una perspectiva de inteligencia

Las ilustraciones de los centros de seguridad cibernética en los Estados Unidos y en Brasil nos dan una idea de la superposición de intereses, autoridades,

y responsabilidades para defender el espacio cibernético. Las preguntas que rodean a un ataque o intrusión son por supuesto numerosas, e incluyen, entre otras cosas: ¿Qué pasó luego de obtener acceso no autorizado? ¿Fue algo alterado o robado? ¿Fue una repetición de un evento anterior? ¿Sabemos cuál fue el código (o herramienta) de acceso a la computadora usado? Los responsables de inteligencia deberían responder a muchas de estas preguntas (u otras relacionadas) para que él o ella puedan gestionar de manera inteligente las acciones de inteligencia necesarias y restringir o prevenir futuros eventos. Las agencias de inteligencia responsables de la seguridad cibernética pueden anticipar la interacción con el conjunto completo de centros en sus respectivos países. La interacción incluirá un intercambio de información mutuo.

Un escenario hipotético ayudará a iluminar la dinámica de un evento cibere-spacial accionable en el diverso contexto del medio ambiente institucional de seguridad cibernética de Brasil y de Estados Unidos. (Para asegurarse de que este es un escenario claramente hipotético, se referirá a los países A, B, C, etc., e individuos o grupos de intrusos cibernéticos 1, 2, 3, etc.) Suponga que un grupo de intrusos (#1) obtuvo acceso no autorizado a un sitio Web gubernamental del país A (y a la base de datos conectada a él). Una vez que ganó acceso, el grupo comenzó a descargar información y a cambiar el sitio Web. El grupo intruso (una mínima alianza que incluye individuos de los países A, B, C, D) luego vendió o entregó algo de información de esa base de datos a otros intrusos (#2, #3, y #4), en los países E y F.

Los cambios del sitio Web parecían solamente alteraciones al principio, pero los investigadores gubernamentales del ciberespacio descubrieron que algunos de los datos fueron destruidos. Los defensores también encontraron dos programas que los grupos de intrusos dejaron: uno entra la información de ingreso de cualquiera que visita el sitio Web automáticamente y la envía a un servidor en el país C. El otro programa trataría de tomar control de cualquier computadora del gobierno cuyo usuario descargaría un archivo en concreto. Los defensores gubernamentales del espacio virtual pudieron desactivar inmediatamente los dos programas que dejaron.

Algunas de las bases de datos contenían información personal de los empleados del gobierno, al igual que de ciudadanos privados; información usada para el desarrollo de políticas gubernamentales, contratos del gobierno con

## Gestión de Inteligencia en las Américas

compañías para el apoyo de la defensa nacional, orden público y servicio de salud nacional y finalmente, información del administrador de sistemas, incluyendo palabras claves que permitían niveles variados de acceso a las bases de datos. Aunque ninguna de las base de datos estaban catalogadas de acceso “clasificado”, algunas de las políticas gubernamentales e información de contratos se encontraban ahí y eran sin duda confidenciales. Los empleados gubernamentales y ciudadanos privados estarían preocupados debido a que su información privada fue accedida sin autorización.

### *Entusiasmo para compartir información de incidentes en ciberseguridad*

Debido a que este escenario entraña una amenaza doméstica y extranjera al gobierno del país A, al sector privado y a los ciudadanos privados, todas las comunidades discutidas en este ensayo necesitarán aprender lo suficiente para proteger sus operaciones futuras en el ciberespacio. Como muestra la discusión, cada una de las cuatro comunidades (de inteligencia, militar, aplicación de la ley, y sector privado) -las cuales, para este ensayo, incluyen la industria de internet en su totalidad- inicialmente tienen sólo conocimiento parcial del caso.

Al ser participantes claves, los responsables de inteligencia querrán saber quién fue el intruso para poder monitorear una futura actividad del actor extranjero que constituye el grupo intruso #1, y de los otros intrusos, idealmente para proporcionar advertencias contra intrusiones futuras. Ellos querrían saber qué pasó — detalles suficientes del ataque para permitirles buscar otras indicaciones y asociaciones que puedan ayudarles a entender por qué la intrusión ocurrió en primer lugar. Ese “qué” en este caso podría ser las herramientas y tácticas que los intrusos utilizaron al igual que los metadatos sobre la información que se encontraba en las bases de datos. La información real dentro de las bases de datos probablemente estaría más allá de la autoridad del responsable de inteligencia para adquirir, pero podría ser accesible para organizaciones de contrainteligencia. Los responsables de inteligencia desearían saber también por qué. Esto les podría dar una mejor perspectiva o una proyección prospectiva del nivel de amenaza a la seguridad nacional.

La comunidad militar, y en particular la inteligencia militar, estaría interesada en el evento por varias razones, especialmente la naturaleza del acceso que

obtuvieron los intrusos a la información de contratos de defensa. Ellos también estarían interesados en por qué los intrusos destruyeron información, así constituyendo la definición de un ataque. Si la comunidad militar es responsable por el CERT nacional más allá de su propia red, entonces la necesidad de información detallada se extiende aún más.<sup>737</sup>

La comunidad de orden público (LE) y especialmente cualquier unidad especializada en desarrollar inteligencia, tiene quizás la necesidad más amplia de información en este escenario. Ellos necesitan saber a quién procesar y qué evidencia puede ser útil para el procesamiento criminal en la corte. La comunidad de orden público necesita detalles sobre qué sucedió para así determinar qué leyes han sido violadas. Ya que hay miembros domésticos y extranjeros del grupo intruso #1, la comunidad de orden público lidiaría con cortes nacionales e internacionales al intentar el proceso judicial. La necesidad de información de la comunidad de orden público sobre los intrusos relacionados puede depender de las leyes cibernéticas en el país A.

La comunidad del sector privado parece tener menos necesidades diversas en este escenario, pero ese criterio inicial puede ser erróneo. Por ejemplo, quiénes son los intrusos puede o no ser importante desde el punto de vista de una reacción inmediata, pero lo que sucedió y por qué sucedió son importantes sin duda alguna. El sector privado en su mayoría, especialmente aquel asociado con contratistas gubernamentales, también quisiera saber qué información fue descargada y de las herramientas y tácticas empleadas. Lo que fue descargado sería importante desde un punto de vista tanto operacional como legal. La información de herramientas y tácticas le permitiría al sector privado prepararse mejor para proteger las redes dentro de su propio ámbito. Dependiendo de ese ámbito (y las leyes del país A), las oficinas de seguridad cibernética del sector privado también podrían necesitar saber algunos detalles sobre la información que fue robada, para poder alertar a aquellos individuos del hecho de la intrusión.

Teniendo el conocimiento de lo que varias comunidades de seguridad cibernética necesitan saber, y por qué, sigue siendo la base crítica para el intercambio de información de inteligencia. Le permite a los responsables de inteligencia, quienes tienden a tener una perspectiva amplia del incidente, saber qué información deben tratar de reunir, que se le puede permitir a ellos saber qué fuentes deben buscar y qué métodos pueden utilizar para obtener

información de aquellas fuentes. Sin embargo, existen impedimentos para la obtención e intercambio de información, que se pueden considerar problemáticos o restrictivos, aun para las agencias de inteligencia nacional.

### *Impedimentos para el intercambio de información en ciberinteligencia*

Claro que los responsables de inteligencia tienen la obligación de reunir información de amplia gama, pero también tienen la obligación de proteger la información que obtuvieron<sup>738</sup> y las fuentes y métodos utilizados para obtenerla. La segunda obligación puede complicar el cumplimiento de la primera. El escenario anterior puede ser utilizado para generar una discusión de algunos aspectos de aquella complicación.

Un responsable de inteligencia eficaz debería asegurar que su organización tenga acceso legal a una variedad de fuentes de información. Parte de esa información puede ser obtenida de manera abierta. Obtener esa información de otras fuentes puede requerir métodos alternativos de carácter clandestino o encubierto. A veces la fuente de información puede determinar el nivel de clasificación e inclusive el modo en el que la información es manejada. A veces la misma información, sin importar los métodos utilizados para obtenerla, determinará la clasificación. Y a veces, es su combinación que puede requerir de una clasificación más alta. Además de las restricciones que acompañan a la clasificación de información, la mayoría de los responsables de inteligencia también encontrarán restricciones al compartirla ampliamente, especialmente fuera de la comunidad de inteligencia.

En el caso del escenario anterior, un organismo de inteligencia puede obtener información de inteligencia sobre quienes formaron parte del grupo intruso #1, al igual que la identidad de los intrusos #2 y #3. Esta información pudo haber provenido de fuentes y métodos que requieren un nivel medio de clasificación al igual que de algunas fuentes que requieren de un más alto nivel de clasificación. El organismo también pudo haber obtenido información sobre las herramientas y las tácticas empleadas por el grupo de intrusos. La información sobre las herramientas y las tácticas pudo haber provenido de las fuentes de más alto nivel; y además la información debe ser tratada a través de medios especiales.

El punto central con respecto a las restricciones de clasificación y diseminación es cuidar la información, las fuentes y los métodos. De este manera, sólo aquellos con acceso al nivel de seguridad apropiado deberían poder obtener la información. En la mayoría de los gobiernos, los consejeros o ministros de seguridad nacional de alto nivel podrían obtener las autorizaciones necesarias para ver toda la información sobre los intrusos #1, #2 y #3, más los detalles de sus herramientas y tácticas. Sin embargo, la información en los más altos niveles de clasificación y autoridad puede no estar disponible para la mayoría de los miembros militares, las comunidades de orden público o del sector privado. Es por eso, como fue sugerido anteriormente, que sería muy útil tener la información sobre incidentes cibernéticos manejada por unidades especializadas de inteligencia de las comunidades militares y LE constituidas por individuos con acceso a información de alto nivel de inteligencia, para asegurar que toda la información potencialmente relevante esté disponible en sus respectivos ámbitos de operación.

Cuando el personal o unidades militares especializadas o de la inteligencia de LE no están disponibles, ¿qué puede hacer un responsable de inteligencia para ayudar a satisfacer las necesidades de información de aquellos sin el necesario nivel de autorización? Una propuesta para contestar esto es descrita en una Directiva de la Comunidad de Inteligencia de Estados Unidos:

La utilidad es maximizada cuando los clientes reciben o pueden descubrir rápidamente y extraer o solicitar inteligencia, información y análisis de modo que la utilicen fácilmente y puedan intercambiar con sus colegas, subordinados, y superiores. WMU [*Write for Maximum Utility*- Redactar para Utilidad Máxima] asegura que la inteligencia, información y análisis son producidos para facilitar su utilidad continua -ya sea en su totalidad o en porciones coherentes- de esta manera habilita la diseminación más extensa e incrementa su uso.<sup>739</sup>

El concepto de WMU realmente describe una meta más que una acción. Otra sección de la directiva se refiere al “saneamiento”, insinuando que esta es una de las acciones que puede cumplir con la meta. La directiva no define “saneamiento”, proceso alusivo a quitar la fuente o método de información que originalmente requería marcación/manejo a un nivel alto de seguridad,

## Gestión de Inteligencia en las Américas

para que la información de inteligencia sea reportada a un nivel más bajo de seguridad. La directiva requiere que “los productos saneados nunca deberán rendir hechos u opiniones de manera inconsistente con sus versiones clasificadas más altas — hechos, opiniones, niveles de confidencialidad, y lenguaje probabilístico deben ser congruentes.”<sup>740</sup> Teniendo todo esto en cuenta, los responsables de inteligencia deberían poder proporcionar los detalles sobre las actividades descritas en el escenario, dependiendo del nivel de acceso de seguridad del destinatario pretendido. Esta técnica se puede aplicar a esfuerzos de intercambio nacional e internacional.

La comunidad de inteligencia puede no tener la autoridad para compartir información de inteligencia con el sector privado. En los Estados Unidos, algunos miembros de la comunidad de inteligencia son autorizados a intercambiar información de inteligencia sólo con otras agencias federales.<sup>741</sup> Hay excepciones a esa restricción, pero la restricción es de todos modos una que los responsables de inteligencia deben considerar, especialmente en vista del peligro que representa la aparición del favoritismo si la información es compartida sólo con algunos y no todos los representantes del sector privado.

Los responsables de inteligencia también pueden enfrentar la oposición de otras comunidades para intercambiar cualquier información que puedan tener con la comunidad de inteligencia. Esta oposición puede ser resultado de la cultura organizacional de las otras comunidades, ya sea por la falta de confianza o la idea de que el conocimiento es poder (y ganancia).

### *El intercambio internacional de información en ciberinteligencia*

Muchas naciones tienen acuerdos específicos para el intercambio de información con otros. La mayoría de los acuerdos son de comunidad a comunidad; ya sea, fuerza militar a fuerza militar, agencia de orden público a agencia de orden público, e inteligencia a inteligencia. Con respecto al escenario presentado, el país A puede tener un acuerdo con el país C para intercambiar información entre comunidades de orden público, pero no necesariamente entre comunidades de inteligencia. El sector privado también intercambia información internacionalmente. De hecho, algunas partes del sector privado son internacionales en sí, con intereses y capacidades de obtención de información en muchas naciones.



Además de acuerdos de nación a nación, muchas naciones adscriben a organizaciones multilaterales. En el escenario, todos los miembros pertenecen a la Organización de Estados Americanos (OAS), la cual ha establecido acuerdos de intercambio de información involucrando a un número de comunidades mencionadas en este ensayo. También tiene una estrategia de seguridad cibernética que resume la importancia del intercambio de información sobre una amenaza y prácticas de seguridad cibernética no sólo dentro de los Estados miembros, sino también con empresas privadas. Esta estrategia fue creada por el grupo de trabajo de la Secretaría de Asuntos Legales de la OAS y específicamente trata un asunto de confianza:

Ya que mucha de la información que CSIRTs [Equipos de Respuesta a Incidentes de Seguridad Informática] tienen que intercambiar es de dominio privado o no sensible, la confianza debe ser desarrollada entre todos los participantes como un elemento esencial de la red hemisférica. Para construir estas relaciones de confianza, CSIRTs deberían ser creados para poseer... una infraestructura segura para manejar información confidencial; la habilidad de comunicarse de forma segura con las partes interesadas; y procedimientos para protegerse contra la diseminación inapropiada de información. Los miembros Estados siempre mantendrán el derecho a decidir el tipo de información que será intercambiada a través de sus CSIRTs designados.<sup>742</sup>

Este documento, y la filosofía que abarca, es un paralelo estrecho al enfoque sugerido anteriormente, a través del cual dentro de un solo país, es útil tener unidades de inteligencia especializadas en las organizaciones militares de inteligencia e inteligencia policiaca para facilitar el intercambio de información de inteligencia sobre incidentes cibernéticos.

### **Explorando posibles mejoras al intercambio de información en ciberseguridad**

La seguridad nacional del espacio cibernético se ha convertido en más que un asunto de “todo el gobierno” – es una preocupación de toda la nación, y como tal supone un desafío mayor para aquellos que necesitan intercambiar información sobre amenazas, específicamente especialistas de inteligencia y

## Gestión de Inteligencia en las Américas

sus responsables. La comunidad de inteligencia es, en la mayoría de las naciones, la entidad líder para el monitoreo del contexto extranjero en el cual intenciones cibernéticas y capacidades de base criminal o ideológicas toman forma. Con esta amplitud de responsabilidades, es lógico que la exploración más a fondo para posibles mejoras en las políticas y prácticas de intercambio de información a través del sistema de defensa cibernética sea asumida desde una perspectiva de inteligencia. Este tipo de exploración es un objetivo de esta última sección del ensayo.

La previa discusión acerca del intercambio de información de inteligencia sobre la amenaza generada por acciones hostiles en el espacio cibernético trató políticas y prácticas actuales, al menos en términos generales. Pero ¿y si los responsables de inteligencia pudieran influenciar aquellas políticas y prácticas? ¿Qué podrían elegir para influenciar? Los siguientes puntos toman en cuenta la idea de que algunos aspectos de estas recomendaciones ya pueden ponerse en práctica, pero también que aún no han sido formalizados o institucionalizados.

1. Incorporar flexibilidad en el proceso de requerimientos de inteligencia. En los Estados Unidos, al menos, el proceso formal de requerimientos de inteligencia funciona bastante bien; establece las demandas del consumidor y busca explicar por qué aquella necesidad es importante y prioritaria. Sin embargo, hay momentos cuando un servicio de inteligencia puede, perfectamente de forma legal, descubrir algo que es de gran importancia, pero que todavía no ha sido identificado como una necesidad. Los procesos de requerimientos de inteligencia deben ser lo suficientemente flexibles para adaptarse a ese escenario.

2. Considerar si la comunidad de inteligencia debería tener la autoridad para monitorear dentro de la sociedad la amenaza de actividades hostiles en el espacio cibernético. Por supuesto, el equilibrio entre la seguridad y privacidad o libertad es un asunto crítico al contestar esta pregunta. La misma sociedad necesitará resolver dónde ese equilibrio puede ser afectado. ¿Puede un responsable de inteligencia influenciar de manera ética y moral la decisión de la sociedad? Quizás – si no hay otra manera más que informar a la sociedad sobre la amenaza y establecer confianza. Parece ser que la comunidad de inteligencia, con sus arreglos existentes de supervisión legislativa y judicial, es la apropiada para ejercer esa autoridad.

3. Tratar al espacio cibernético como un dominio culturalmente distinto. “Cambiar la cultura” del intercambio de información dentro de la burocracia es una de las cosas más fáciles de decir y probablemente una de las más difíciles de cumplir. Una de las cosas que los responsables de inteligencia pueden hacer es asegurarse que intercambien lo que las leyes, las políticas y las regulaciones permiten. Otra cosa que los responsables de inteligencia deben hacer es explicar, en términos claros, por qué pueden o no compartir información:

- Qué compartir (¿y en qué nivel de seguridad)? En los Estados Unidos, la política actual establece qué información debe ser clasificada, cómo debe ser manejada y quién la puede ver. Un tema, para algunos, es si las leyes y reglas existentes están siendo aplicadas apropiadamente a la inteligencia relacionada con el ciberespacio. Al menos una autoridad opina que el rol de la inteligencia en el ciberespacio necesita ser definido e implementado de manera diferente. El General Michael Hayden, antiguo Director de la Agencia de Seguridad Nacional y de la Agencia Central de Inteligencia, recomienda que formulemos una serie de preguntas difíciles sobre la seguridad cibernética y la protección de la información en este dominio. Por ejemplo, “¿qué constituye para el siglo veintiuno una expectativa razonable de privacidad?”<sup>743</sup> En este contexto, los responsables de la inteligencia podrían beneficiarse de una reevaluación general del concepto de privacidad e información privada en el espacio cibernético, como dice el General Hayden “Google y Facebook saben mucho más sobre la mayoría de nosotros en comparación con lo que nosotros compartimos con el gobierno.”<sup>744</sup>
- ¿Con quién compartir? Hay un incremento de posibles clientes para la información de inteligencia relacionadas con las amenazas del espacio cibernético:
- Las restricciones actuales prohíben a los responsables de inteligencia intercambiar información directamente con ciertos clientes (Estado federal, policías locales o intercambios con grupos de indígenas). Mientras haya buenas razones porque esto debería ser el caso para la mayoría de la inteligencia (incluyendo debates no resueltos sobre los derechos del gobierno federal vs. los de los estados,

## Gestión de Inteligencia en las Américas

y sobre quién paga o quién regula qué), creemos que respecto a las amenazas en el ciberespacio, la situación es diferente. Los límites físicos no significan mucho en el ciberespacio, y la lógica de la simetría sugiere que una defensa sensata contra las amenazas cibernéticas igualmente no tendrían que ser restringidas geográficamente mediante, por ejemplo, una diferenciación entre amenazas internas y externas.

- Compartir información de inteligencia entre miembros del sector privado es muy difícil de hacer, y puede estar prohibido en algunas instancias. La razón puede ser entendible: el problema de cómo evitar mostrar favoritismo, la existencia de diferencias en la confianza de algunos establecimientos sobre otros, y demás. Sin embargo, una sinergia importante será obtenida cuando los responsables de la inteligencia puedan intercambiar información con el sector privado y el gobierno federal por igual. La Senadora de Estados Unidos Dianne Feinstein envió recientemente una carta al Presidente Obama recomendando un cambio en esta área. La carta incluyó un llamado para una Orden Ejecutiva que “dirigiría a la Comunidad de Inteligencia y el Departamento de Seguridad Interna a proporcionar la mayor cantidad de información posible al sector privado sobre amenazas cibernéticas, incluyendo información clasificada”.<sup>745</sup> La prensa de Estados Unidos indicó que el Presidente iba contemplando la acción ejecutiva.<sup>746</sup> De manera similar, la Sede de Comunicaciones del gobierno británico ha desarrollado un programa llamada “Seguridad Cibernética para Negocios” según se ha reportado. Una de sus metas es establecer el intercambio cooperativo de información entre la inteligencia británica y el sector privado británico.<sup>747</sup>

- Compartir información de seguridad cibernética de manera multilateral, nunca ha sido una decisión fácil, y debería ser apoyada por una claridad en las reglas para el intercambio interno dentro de países. El objetivo puede ser entendido y promovido al tratar a continuación la pregunta final.

4. Identificar una agencia existente de inteligencia, orden público o defensa o crear a una nueva para centralizar la seguridad y defensa del ciberespacio a lo largo de los dominios públicos y privados. De hecho, para cualquiera que

lidia con la amenaza de acción hostil en el ciberespacio, sabiendo quien está a cargo de la recopilación de información, su análisis y su uso para la identificación de amenazas cibernéticas y el apropiado proceso judicial es casi imposible, debido a las tantas comunidades nacionales, cada una con diferentes responsabilidades y jefes. Si los responsables de inteligencia pudieran influenciar cualquier política y prácticas del poder ejecutivo, debería ser aquí. Ya sea la comunidad de orden público, inteligencia o defensa, alguien debe estar a cargo. Las leyes, órdenes ejecutivas, guías de políticas y regulaciones necesitan ser escritas y poner a una sola entidad a cargo para que todas las comunidades puedan identificar sus roles a la hora de defender su nación y sus aliados.

En cualquier país, la entidad necesitaría tres conjuntos de autoridades/responsabilidades (o su equivalente): inteligencia extranjera, orden público, y regulador (que fije las reglas). En los Estados Unidos, una organización que tiene este conjunto de autoridades y responsabilidades es la Guardia Costera de Estados Unidos. Quizás esa organización, de la manera que gestiona sus responsabilidades de inteligencia, orden público y regulación, podría servir como un modelo para la organización de seguridad del espacio cibernético. La Guardia Costera fue eficaz en combinar las capacidades de inteligencia junto con las responsabilidades de aplicación legal y reglamentos durante la Era de la Prohibición en la historia de los Estados Unidos, cuando un alto volumen de bebidas alcohólicas ilegales entraron a los Estados Unidos de contrabando desde barcos cercanos a la costa, una actividad coordinada por grupos del crimen organizado.<sup>748</sup>

De igual importancia, la entidad necesitará establecer y mantener confianza entre los ciudadanos de los Estados Unidos:

- Confianza en que la privacidad personal y seguridad nacional puedan ser complementarias en práctica, en vez de estar siempre en desacuerdo, con ideales separados y en competencia. Esto tendrá que ser una vía de doble sentido. La sociedad debe determinar si puede confiar en que el gobierno monitoree ciertas actividades en el ciberespacio hasta los mismos niveles donde el sector privado de hecho ya monitorea. El gobierno (especialmente las partes responsables por la seguridad del espacio cibernético) debe mantener la confianza de la sociedad que protegerá la privacidad como es establecida por las leyes que la sociedad acepta.

## Gestión de Inteligencia en las Américas

- Confiar en que el gobierno y el sector privado puedan trabajar juntos para intercambiar información. Esto también es una vía de doble sentido. El gobierno debe confiar en que el sector privado proteja la información confidencial. El sector privado debe confiar en que el gobierno protegerá la propiedad intelectual y la información confidencial. Ambos deben confiar en que utilizarán el intercambio de información para propósitos previstos y autorizados por la ley y la política.

### Biografía del autor

**Robin M. Rogers** posee un título de posgrado en Inteligencia Estratégica de la Universidad de Inteligencia de Defensa (ahora la Universidad Nacional de Inteligencia - UNI) y otro título de posgrado en historia de la Universidad de Maryland. Sirvió en la Fuerza Aérea de los Estados Unidos durante 30 años, jubilándose como Coronel. Posteriormente, trabajó para el Departamento de Defensa en inteligencia como analista y maestro de análisis antes de hacer transición a una posición de política corporativa. En la actualidad, se encuentra laborando en la UNI, donde utiliza su experiencia combinada en inteligencia, cibernética y política para desarrollar el currículo relacionado con las operaciones de ciberespacio para la universidad. Email: Rogers@dodiis.mil.



© Este ensayo copyright 2014. Todos derechos reservados.

**Captar el Capital Intelectual del Sector de Seguridad:  
Transformar la Conciencia del Entorno del Asesor  
en un Entendimiento Socio-Político dentro de un  
Ambiente de Poder Inteligente (“Smart Power”)**

William S. Brei  
Nathalie J. Frensley  
Killaurin O. Roberts

*Mientras que este “Apogeo Afgano” comienza a declinar y más restricciones financieras y políticas entran en vigencia, vamos a tener que ser imponentes dar poderes a los mentores como una organización. Sus ventajas sociales tácticas con sus homólogos tendrán que ser fusionadas en impactos operacionales reales. De otra manera, las metas estratégicas de la Alianza se convertirán en una situación delicada como la cáscara de un huevo y las naciones comenzarán a acusarse el uno al otro.*

— Mentor Operacional de la OTAN y Comandante del Equipo de Enlace, Comentarios durante la Noche de Cigarros, Octubre del 2010, Afganistán.

Los comentarios informales del Comandante destacan las complejidades que enfrentan todas las misiones de asesoramiento desde el nivel de distrito al nivel ministerial, en el entorno de “Poder Inteligente” en Afganistán. Estas complicaciones, como se explican en adelante, se derivan de problemas de soberanía por parte del país anfitrión tanto como de los países donadores, que por un lado intensifican la necesidad de entender mejor el ambiente socio-político de los países anfitriones y que por otro lado se crean otros obstáculos y fuertes restricciones al lograrlo. En este trabajo, presentamos el concepto del Equipo de Red Socio-político y Análisis de Comportamiento (SNBAT), utilizado en Afganistán desde el 2010 hasta principios del 2012, en apoyo a una misión multinacional, a un campo de asesoramiento al nivel ministerial encargado de construir las capacidades y las aptitudes de las Fuerzas de Seguridad Nacional de Afganistán (ANSF).<sup>749</sup> Se ofrece el concepto SNBAT como una estrategia y modelo de reforma para el uso de las misiones de asesoramiento en el sector de seguridad, con la finalidad de mejorar el entendimiento socio-político



acerca de sus países anfitriones contrapuestos, dentro del ambiente de hoy políticamente cargado de “Poder Inteligente”.

Especialmente en estos ambientes multilaterales de Poder Inteligente, se ve una tendencia de las naciones anfitriones asesoradas de tener relaciones y acciones políticas relativamente independientes y autónomas, de acuerdo con sus afirmaciones de la importancia de mantener su soberanía.<sup>750</sup> Como explicamos abajo, el éxito de las misiones de asesoramiento depende del entender el ambiente socio-político que afecta la nación anfitriona. En tiempos anteriores, habrían sido los órganos de inteligencia los que proveerían información al equipo de asesoramiento para el desarrollo de su conciencia del ambiente local. Pero, como veremos, la aplicación de la política conocida como Poder Inteligente nos ha llevado a la coyuntura donde estos órganos de inteligencia se encuentran ante restricciones adicionales a sus acciones. Esto se debe en parte al énfasis en la soberanía de la nación anfitriona, pero también son contribuyentes las dificultades de la coordinación multinacional de inteligencia. Además, la naturaleza sensible de la misión de asesoramiento impide a las organizaciones de inteligencia proveer o aparentar el suministro de información socio-política detallada o análisis para los asesores, dado el miedo de perder la confianza de los colegas del país anfitrión. Por lo tanto, el cuerpo de asesores en un ambiente de Poder Inteligente necesita solucionar el problema de cómo cumplir sus necesidades apremiantes de entendimiento de la situación en una misión que requiere compromiso cara a cara con altos representantes del país anfitrión.

Nosotros confrontamos este problema dentro del encuadramiento del capital intelectual. Captar, recopilar, desarrollar y preservar el capital intelectual de una organización son los medios para transformarla en una organización de aprendizaje. La estrategia de SNBAT, en un contexto de misión de asesoramiento, es aplicar la administración estratégica del capital intelectual para permitir que una misión de asesoramiento realice las funciones de inteligencia que han sido tradicionalmente militares y civiles sin los riesgos negativos de una misión que acompañan la participación en una burocracia centralizada de inteligencia. La naturaleza de SNBAT, que opera completamente y solamente dentro de la misión de asesoramiento, ayuda a asegurar la confidencialidad de las relaciones que son simultáneamente personales y profesionales para los asesores, aun cuando el equipo combina información individual del asesor para crear un vistazo general coherente del ambiente socio-político de la misión del asesor.

## Gestión de Inteligencia en las Américas

Los autores extraen de sus experiencias con el Desarrollo del Ejército Nacional Afgano (ANA DEV), un elemento multinacional de asesoramiento ministerial de la OTAN, Misión de Entrenamiento - Afganistán (NTM-A), para sugerir cómo las misiones de asesoramiento en ambientes de Poder Inteligente pueden crear una capacidad *orgánica* de administración de capital intelectual para captar, preservar y combinar coherentemente los conocimientos y experiencias socio-políticas de los asesores y mejorar la eficacia de la misión. Al competentemente conectar los puntos desconectados, al captar el conocimiento en contexto, al entregar información y conocimiento directamente al punto de ejecución, y al adoptar un largo punto de vista histórico -los cuatro elementos del desarrollo de capital intelectual del ANA-DEV SNBAT- se construye un entendimiento socio-político de conciencia del entorno del asesor.

### Poder inteligente y la demanda de análisis socio-política en ambientes de asesoramiento militar

Las Fuerzas Especiales de Estados Unidos se han responsabilizado históricamente de asesorar a las fuerzas de seguridad extranjeras. Una consecuencia reciente del ascenso del Poder Inteligente en la política de seguridad nacional y extranjera de los Estados Unidos es el aumento de participación de las fuerzas convencionales<sup>751</sup> en el asesoramiento de la Reforma del Sector de Seguridad (SSR), particularmente a niveles de fuerzas de seguridad nacional (ministerial).<sup>752</sup>

El Poder Inteligente “enfatisa la necesidad de un ejército fuerte, pero también invierte fuertemente en alianzas, asociaciones, e instituciones de todos los niveles para expandir la influencia estadounidense y establecer la legitimidad de las acciones estadounidenses.”<sup>753</sup> El enfoque del Poder Inteligente combina los tipos de poderes “duros” de coerción e inducción por un lado, con tipo de poderes “blandos” de atracción y co-opción, por el otro.<sup>754</sup> El énfasis de Poder Inteligente en las alianzas, las asociaciones, e instituciones, requiere considerar la soberanía nacional no tanto en términos relativos de ganancia (de suma cero; gana uno, pierde otro) sino más en términos absolutos de ganancia (suma variable; ganan ambos).<sup>755</sup>

Desarrollo del Sector de Seguridad -la gama completa de actividades que asume una nación y sus asociados para mejorar la manera de proporcionar

protección, seguridad y justicia a sus ciudadanos<sup>756</sup>- es una clave de la actividad del Poder Inteligente.<sup>757</sup> La reforma del sector de seguridad restablece o reforma las “*instituciones* y las posiciones *ministeriales* claves que mantienen y proporcionan supervisión para la protección y seguridad de la nación anfitriona y su gente” (nuestro énfasis).<sup>758</sup> El *asesoramiento* de sector de seguridad particularmente a nivel ministerial, enfatiza el lado blando del Poder Inteligente porque los asesores deben “articular las sugerencias a sus...contrapartes persuasivamente” en vez de “directamente implementar cambios necesarios para el SSR.”<sup>759</sup> Ciertamente, el éxito de los “asesores depende de su habilidad de dar recomendaciones de manera que los cambios sean aceptables para aquellos que asesoren.”<sup>760</sup>

El Poder Inteligente tiene tres componentes: fusión de poderes militares, diplomáticos y de desarrollo,<sup>761</sup> promoción de democracia y una economía de mercado,<sup>762</sup> y participación en operaciones multilaterales con aumento de participación de las Naciones Unidas.<sup>763</sup> Cada componente afecta al ambiente de operación de asesoramiento del Sector de Seguridad. El asesoramiento del Sector de Seguridad se realiza en un ambiente de promoción de democracia, típicamente donde un gobierno responsable y transparente ha sido quebrado y donde la construcción de democracia tal vez no sea popular con los intermediarios influyentes locales. En Afganistán, el multilateralismo del Poder Inteligente sucede dentro de la estructura de la alianza de la OTAN, la cual al mismo tiempo opera bajo un mandato de las Naciones Unidas. Varias requisitos únicos<sup>764</sup> complican el comando y la coordinación de las misiones multinacionales de asesoramiento.<sup>765</sup> El desarrollo del Sector de Seguridad sucede en conflicto, posconflicto y/o ambientes de estado débil donde el ejército de la nación anfitriona y autoridades civiles coordinarían planes y actividades junto a oficiales militares, diplomáticos y de desarrollo de la comunidad internacional quienes coordinarían sus acciones igualmente.<sup>766</sup>

## Gestión de Inteligencia en las Américas

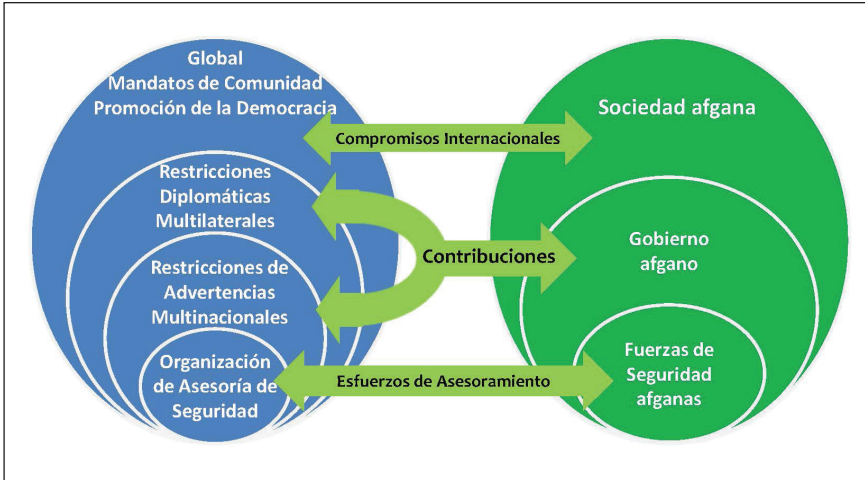


Figura 15. El Ambiente Operacional Complejo de la Misión de Asesoramiento

Fuente: Creado por los autores.

El Poder Inteligente expande el ámbito y nivel de entendimiento que los asesores del sector de seguridad ministerial necesitan sobre el ambiente socio-político y de comportamiento en el cual trabajan. Algunos elementos específicos de ese ambiente incluyen:

- Las historias individuales de sus homólogos y sus relaciones formales e informales con la organización de seguridad de la nación anfitriona;
- El historial de la organización de seguridad y las relaciones formales e informales dentro de las estructuras más amplias de poder gubernamental, incluyendo otros ministerios gubernamentales y unidades;
- La historia social y las relaciones dentro y entre los grupos sociales, incluyendo a los actores de la sociedad civil, económica y religiosos.

El rostro humano de estos requerimientos generales es ilustrado en las siguientes historias.

Un asesor estaba frustrado sobre la cantidad de tiempo que su colega pasaba en reuniones con individuos fuera del Ejército Nacional Afgano (ANA) y el Ministerio de Defensa (MoD). El colega había pasado casi la mayoría de su carrera militar en una de las escuelas de entrenamiento del ANA, comenzando antes de la guerra Afgana-Soviética. Su historial de carrera le dio la habilidad única de averiguar reclamos de ex muyahidines quienes buscaban unirse al ANA en rango acreditado basándose en su servicio previo a la guerra Afgana-Soviética. Cuando esto fue llevado a la atención del asesor, se hizo claro que las “visitas sociales” del General para discutir eventos que ocurrieron hacia más de tres décadas, de hecho fueron deberes importantes para asegurar el profesionalismo, dada la pérdida de los expedientes oficiales durante uno de los tantos conflictos de Afganistán. El asesor ahora también se dio cuenta que este General era una fuente única para entender la historia y evolución de la doctrina, maniobras y entrenamiento de ANA.

La Fuerza Internacional de Asistencia de Seguridad (ISAF) insistió que un individuo con muy buenas conexiones en el centro de un escándalo público debiera de ser removido de sus deberes, y le fue asegurado que eso ocurriría. Un analista fuera del ANA-DEV escribió un informe de amplia circulación alegando que un líder del MoD era participante del escándalo debido a su aparente lentitud para cumplir con esas garantías. El analista no tuvo en cuenta que el líder del MoD, de la misma etnicidad que el individuo que fue removido del servicio, estaba asegurando el apoyo de los ancianos del clan para la remoción del último y así previniendo las apelaciones a las lealtades de los clanes para revertir la decisión. Además, el líder del MoD y el individuo a ser removido estaban en diferentes facciones políticas dentro del grupo étnico. Adicionalmente, el analista no tomó en cuenta que las normas sociales Afganas previenen el “despido” de un colega que es par en estatus o un compatriota étnico; sin embargo, se permite moverlos lateralmente a otra posición.

Una contraparte había sido degradada a una posición menor dentro del MoD unos años antes por el presidente, haciendo que los asesores principales ya no lo reconocían como un jugador poderoso en el liderazgo militar. El asesor actual averiguó, sin embargo, que este individuo era el anciano superior de una tribu históricamente influyente. Investigaciones adicionales sugirieron que a lo largo de la historia moderna de Afganistán, un número desproporcionadamente alto de sirvientes civiles fueron extraídos de esta tribu. En esta instancia, el estatus influyente de la contraparte eclipsó y compensó robustamente, por lo que fue una degradación en la oficina solamente.

Los conocimientos socio-políticos permiten un entendimiento de razones que pueden estar detrás de las acciones de un contraparte que parece no tener propósito salvo obstaculizar y retrasar. Dicho conocimiento también apunta a “influyentes” que “pueden lograr resultados” dentro de una estructura de autoridad que permanece oculta ante un forastero. En resumen, los asesores con entendimiento extenso del ambiente operativo, al contrario de la conciencia superficial de las convenciones culturalmente apropiadas de compromiso sociales, son capaces de sacar provecho al conocimiento social.

### **Sobre ratones y ratoneras: Entender las necesidades de administración de información y conocimientos únicos de la misión de asesoramiento**

Cuando fue creado, el ANA-DEV asimiló varias organizaciones que durante décadas anteriores habían contribuido al asesoramiento y a la orientación del Ministerio de Defensa Afgano (MoD).<sup>767</sup> Los planes trimestrales de desarrollo ministeriales individualizados producidos por asesores (MDPs) con objetivos definidos, logros, y medidas de éxito, fueron establecidos para monitorear y evaluar el progreso hacia la profesionalización de las oficinas de asistentes ministeriales, secciones del personal, y unidades especiales del MoD Afgano.

Como parte de las evaluaciones trimestrales, se esperaba que los asesores produjeran lo que era conocido como “Mapas de Terreno Humano” sobre sus contrapartes. Los asesores del ANA-DEV tenían extensa información y conocimientos sobre el ambiente socio-político. Sin embargo, los asesores no tenían información y análisis para apoyar o corroborar su conocimiento en un profundo contexto histórico y/o en relación a las redes sociales de los

ambientes contemporáneos a veces cambiantes – políticos, sociales o religiosos. Además, los “Mapas de Terreno Humano” fueron restringidos a una sola diapositiva y estructurados para producir tablas de “ego” sin red o representaciones diagramáticas Venn de información de amplios grupos sociales variados. Se perdieron las oportunidades para combinar la conciencia del asesor individual de las partes del ambiente socio-político de su contraparte en un entendimiento más amplio de la situación organizativa de la misión de asesoramiento del MoD Afgano como una organización de seguridad profesionalizada, como una organización de seguridad dentro de un ambiente gubernamental político, y como una organización de seguridad gubernamental potente políticamente.

Peor que la pérdida de oportunidades que resultan de la falla del “Mapeo de Terreno Humano”, fue la evaporación del conocimiento de los asesores y su influencia con sus contrapartes ya que su servicio militar se terminó. En ese momento, el ANA-DEV no tenía capacidades de administración de conocimiento en sitio para captar y retener su información socio-política y de comportamiento único. Sin la captura y retención de la información del asesor, un cuerpo de corporación de conocimiento de asesoramiento no podría ser desarrollada para los asesores de segunda, tercera y cuarta generación. Las contrapartes afganas vieron por sí mismas la falta general de conocimiento corporativo acumulado y reconocieron el nivel débil de conciencia de principiante de sus realidades socio-políticas por parte de la mayoría de los nuevos asesores. Desde la perspectiva de asesoramiento, para utilizar la analogía de ratón y ratonera, ANA-DEV no buscó captar y retener información con el propósito de construir una ratonera como sería el caso de una organización formal de inteligencia; sino que, ANA-DEV vio el posible capital intelectual de sus asesores como un medio para construir un ratón más perseverante e informado en un ambiente cambiante y turbulento.

### La singularidad de la información de la relación de asesoramiento

Los asesores individuales de ANA-DEV típicamente pasaron un año en Afganistán. Durante ese año, un asesor pasaría entre 15 y 40 horas por semana con sus homólogos, dependiendo de la intimidad de la relación. A veces los asesores viajaban con sus homólogos. Algunos asesores entablaron diálogos basados en el respeto demostrado al haber hecho un esfuerzo para avanzar

## Gestión de Inteligencia en las Américas

más allá de la competencia elemental en los idiomas Darii o Pashto. El tiempo amplio que un asesor del ANA-DEV pasaba típicamente con una contraparte proporcionó tremenda visibilidad y oportunidad para ganar conocimientos sobre las tendencias de comportamiento y decisiones de un solo individuo, influenciado por eventos históricos, influencia política, y membresía de facción y grupos dentro de la MoD y ANA, Gobierno de la República Islámica de Afganistán (GIROA) y la amplia sociedad afgana. Los pocos que sirven en Afganistán, incluyendo analistas de inteligencia que trabajan en la gran Base de Operaciones Avanzadas (FOBs), tienen tanta visibilidad y tiempo de contacto con superiores afganos como los asesores a las Fuerzas de Seguridad Nacional Afgana (ANSF) en los Ministerios de Defensa y del Interior.

El trabajo diario de un asesor proporcionaba acceso al conocimiento disponible gratuitamente, aunque singularmente único, sobre su contraparte individual. Por ejemplo, los asesores a veces trabajaban con sus contrapartes en desarrollar políticas. Las políticas del MoD tienen ambas firmas y espacios para la firma. Las líneas de firma del Ministro del MoD pueden proporcionar, a aquellos dispuestos a traducir de Darii o Pashto, un nombre completo, del cual es posible identificar no sólo la familia pero también afiliaciones sub-tribales y tribales o clanes, logros académicos, preferencias en formas de dirigirse, y a veces comandos u oficios que se tienen. En algunos casos, el espacio de firma contenía declaraciones sobre acciones y aspiraciones. Además, debido a que los espacios de firma eran escritos por la contraparte afgana, ellos sirvieron como una “presentación social propia”<sup>768</sup> en maneras que los currículos convencionales no podrían hacerlo.

La singularidad del conocimiento de un asesor viene de la obtención y retención de la confianza de su homólogo. Esto conlleva a dos consecuencias. Primero, los conocimientos desarrollados de una relación de asesoramiento los hace intrínsecamente sensibles, pero no por la naturaleza de un conocimiento cualquiera. Más bien los conocimientos del asesor son intrínsecamente sensibles, debido a que si su contraparte percibe una falta de discreción por parte de su asesor, la confianza y el respeto en su relación se erosionaría. Segundo, una consecuencia relacionada es que muchos asesores, aunque ansiosos en analizar el ambiente socio-político y el rol de su contraparte en él, resiste el compromiso con organizaciones de inteligencia por preocupación sobre cómo la información incluida en su diálogo será utilizada fuera de la misión



de asesoramiento. Muchos asesores en NTM-A identificados por sí mismos como “Correctores, No Recopiladores” y sus evasiones de organizaciones de inteligencia, se intensificaron mientras el episodio infame de Wikileaks se desarrollaba.

### Desempacar el problema: La administración estratégica del capital intelectual de los asesores

Cuando mentores y asesores, tales como Comandantes del OMLT, aseguraron que las “ventajas tácticas sociales...tendrán que ser fusionadas en impactos operacionales reales”, el liderazgo del ANA-DEV entendió que esto significa recopilar la conciencia y conocimiento de un asesor individual en un entendimiento completo del ambiente organizativo, socio-político y de comportamiento del MoD. El liderazgo del ANA-DEV no vio el hueco del entendimiento completo como un problema causado por la falta de aprendizaje y la aplicación de principios y técnicas de asesoramiento, el inicial conocimiento de cada país específico, o la experiencia en Afganistán por parte de los asesores. Muchos miembros de servicio uniformado que asesoraron, completaron múltiples periodos de servicio en Afganistán. Muchos asesores contratistas habían pasado tres años o más en Afganistán. El liderazgo del ANA-DEV había valorizado altamente el conocimiento que los asesores trajeron de su preparación antes de su despliegue, incluyendo el extensivo entrenamiento en idiomas e información específica del país dado a “*Afganistán-Pakistán Hands*” (APH) y a los asesores del Ministerio de Defensa (MoDA).<sup>769</sup> Muy al contrario, el liderazgo del ANA-DEV, en las palabras del coronel canadiense, entendió que “demasiada información desorganizada y sin poder utilizar ésta hecha por los asesores, en vez de proveer menos información, está previniendo que la misión de asesoramiento se convierta en una organización de aprendizaje.”

Desde el aumento de conocimientos e información de economía a mediados de los años 90, el manejo estratégico del capital intelectual y el aprendizaje organizativo han sido reconocidos como central para la competitividad de una organización y para cumplir con sus metas eficientemente. La introducción de un volumen influyente sobre el capital intelectual nota que

en parte, el desafío de la administración es orquestar la transformación de materia prima intelectual generado por

## Gestión de Inteligencia en las Américas

individuos a capital intelectual – conocimientos recopilados de manera que puedan ser invertidos directamente en el mismo sentido como los activos de una empresa... Las organizaciones poseen depósitos inmensos no estructurados de información informal, en los cuales la ausencia de programas de capital intelectual es distribuida de manera casual por la mente de individuos y una plétora de medios de registro de datos tales como memos, libros, mensajes de voz, archivos y bases de datos. E inclusive activos intelectuales menos tangibles están incluidos implícitamente en el trabajo de la organización misma – en su cultura y en sus rutinas y procesos informales. Al formar capacidades intelectuales más deliberadamente desde este mar de material intelectual sin estructura, la administración puede más fácilmente invertir dicho capital en oportunidades con el objetivo de cumplir requerimientos estratégicos de conocimiento.<sup>770</sup>

El capital intelectual y el aprendizaje organizativo están separados pero son componentes relacionados de adaptación organizativa a un ambiente externo impredecible. Cuando un proceso para convertir la capacidad intelectual en capital organizativo está siendo utilizado, una organización de aprendizaje puede surgir. Dicha organización facilita el aprendizaje por sus miembros y se transforma continuamente.<sup>771</sup> Lo hace al captar el conocimiento generado por sus diferentes componentes a nivel operativo y forjando esos conocimientos en información corporativa compartida a lo largo de la organización.

La administración estratégica del capital intelectual, para fomentar una organización de aprendizaje, tiene tres características generales. La primera es “conectar a lo desconectado” al proporcionar una fundación de información para “crear y conectar a comunidades....con intereses y tareas similares.”<sup>772</sup> En un contexto de asesoramiento, esto involucra recopilar la información y conocimiento de cada asesor derivado de cada relación individual de asesoramiento en un entendimiento general del ambiente de asesoramiento de la misión. Cuando esto se logra, los asesores empiezan a mejorar su entendimiento de los sistemas y procesos más grandes que restringen las acciones de sus homólogos.

La segunda es facilitar “la captura del conocimiento en contexto... [porque las organizaciones] pragmáticamente no pueden...requerir que los profesionales

aborden preguntas generales sobre su conocimiento como un proceso fuera del flujo de trabajo normal. [Las organizaciones] necesitan acumular...conocimiento que representa sus contextos particulares....”<sup>773</sup> Cuando se aplica al asesoramiento, esto significa que el capital intelectual de una misión debe tener competencias y debe mantener conocimientos de políticas actuales sobre la institución de seguridad, el proceso de asesoramiento, y de las interacciones entre los dos, al igual que tener conocimiento sobre el ambiente socio-político más amplio de la institución de seguridad.

El tercer elemento de la administración estratégica promueve que la organización de aprendizaje “capte el capital intelectual en contexto [y] enviándolo directamente al punto de ejecución. El capital intelectual formado e invertible tiene relativamente poco valor, a menos que sea enviado donde y cuando sea necesario.”<sup>774</sup> Para una misión de asesoramiento, esta tercera característica subraya la necesidad de que la capacidad de capital intelectual se origine desde adentro y que se dedique al asesoramiento de misiones con el propósito de asegurar su valor para el aprendizaje organizativo.

Un cuarto elemento adicional que promueve el aprendizaje organizativo es la recopilación del conocimiento institucional histórico de la organización, además de su conocimiento actual. Diferentes organizaciones cuentan con una variedad de metas y necesidades estratégicas, algunas -tales como misiones de asesoramiento- tienen que estar al lado extremo de la adaptación a cambios ambientales externos. Para las misiones de asesoramiento, esos cambios pueden incluir políticas domésticas en el país de origen del asesor, políticas de alianza/coalición, y políticas de la nación anfitriona al igual que la evolución de la profesionalización y la capacidad del homólogo de la institución de sector de seguridad. En el ambiente altamente incierto de una misión de asesoramiento del sector de seguridad, las necesidades de aprendizaje organizativas de esa misión serán más parecidas a aquellas organizaciones que enfrentan una renovación estratégica. Un contexto de renovación estratégica coloca necesidades adicionales en una organización de aprendizaje, requiriendo la renovación de “organizaciones para explorar y aprender nuevas formas mientras simultáneamente aprovechando lo que ya han aprendido.”<sup>775</sup>

Para una misión de asesoramiento comprometida en asesorar reacciones “normales” versus las “abnormales” a cambios en ambientes turbulentos, su requerimiento de conocimientos demanda que su capacidad para manejar

su capital intelectual tome una perspectiva histórica relativamente larga al contextualizar y recopilar el conocimiento del asesor. Por esto y por las tres razones previas, es muy poco probable que una entidad de afuera de la misión de asesoramiento pudiera administrar exitosamente el capital intelectual de tal manera que pueda contribuir para volver a formar la misión en una organización de aprendizaje.

### **Construir el capital intelectual del ANA-DEV: Cómo la conciencia del entorno del asesor es orgánicamente transformada en un entendimiento socio-político de la misión de asesoramiento**

La pregunta central que el ANA-DEV enfrentó al convertirse en una organización de aprendizaje se redujo a “Cómo se puede crear un entendimiento eficaz del ambiente socio-político del MoD de la conciencia del entorno poseído por la combinación de asesores individuales, particularmente en un contexto de datos e información abundante?” Aunque preguntas similares son centrales al trabajo de muchos profesionales, incluyendo los académicos y los trabajadores en desarrollo, quizás no es sorprendente que esta pregunta ha sido estudiada intensivamente en el mismo contexto del análisis de inteligencia. La Publicación de la Doctrina Conjunta 2-00 (JDP 2-00) “Entendimiento y Apoyo de Inteligencia para Operaciones Conjuntas” del Ministerio de Defensa del Reino Unido, ha lidiado más directamente al tratar de responder doctrinalmente esta pregunta fundamental.<sup>776</sup> No obstante, como se explica abajo, la combinación de las necesidades únicas de asesoramiento y los límites en el análisis de inteligencia previene que inclusive aún esta dirección emergente y valiosa cumpla con las necesidades de la misión de asesoramiento en ambientes de Poder Inteligente.

JDP 2-00 marca al entendimiento como “referencia a la adquisición y el desarrollo de conocimiento para obtener una perspectiva (saber por qué algo ha sucedido o está sucediendo) y visión (ser capaz de identificar y anticipar lo que puede pasar).<sup>777</sup> Lograr el entendimiento exige nuestro “desarrollo de la perspectiva más inclusiva de un actor, grupo, ambiente, o situación.”<sup>778</sup> La conciencia del entorno, “la apreciación de lo que se está pasando, pero no necesariamente por qué se pasa”,<sup>779</sup> necesariamente viene primero, pero por sí mismo permanece como un paso insuficiente hacia adquirir entendimiento. Sin embargo, podemos observar que un “análisis de la conciencia del entorno brinde una gran comprensión (conocimiento) del problema.”<sup>780</sup> Con una

comprensión temprana del problema, “la opinión basada en el conocimiento completo”<sup>781</sup> (en el sentido de ser capaz de estimar relaciones lógicas entre causas y consecuencias del problema) puede proporcionar la previsión que lleva a ser capaz de identificar escenarios anticipados.

JDP 2-00 distingue el entendimiento desde la conciencia del entorno al atribuir a entender un “nivel de análisis y profundidad de comprensión que permite que la opinión sea aplicada eficazmente.”<sup>782</sup> Aplicar este concepto a una misión de asesoramiento requiere dos modificaciones menores. Estas modificaciones se aplican a las limitaciones de cualquier apoyo de análisis fuera de la misión de asesoramiento para cumplir con la información socio-política de la misión de asesoramiento y sus necesidades de entendimiento.

Primero, cuando una misión de asesoramiento se compromete con una institución ministerial, mediante sus numerosos asesores, está en realidad secuencialmente comprometida con sus respectivas contrapartes individuales. Consecuentemente, los contextos de misión de asesoramiento incluyen múltiples contrapartes que hacen parte de la red social o de otra manera se agrupan entre ellos pero cada uno tiene un asesor con una concentración exclusiva en ellos. Para entender las redes sociales y los grupos dentro del ministerio asesorado, hay una necesidad de un ámbito de comprensión integral - una fusión de las perspectivas de todos los asesores - además de la profundidad identificada y enfatizada por JDP 2-00. El ámbito de comprensión, además de la profundidad de comprensión, nos retorna a la necesidad del capital intelectual de conectar a lo desconectado y tomar el punto de vista histórico largo.

Segundo, JDP 2-00 pone énfasis en identificar el nivel apropiado de análisis. Sin embargo, para que este concepto sea relevante para una misión de asesoramiento, hay una necesidad de múltiples niveles de análisis para poder entender mejor a las simultáneas influencias gubernamentales, organizativas y sociales del ministerio en el comportamiento de una contraparte individual. Esto corresponde al principio del capital intelectual de captar el conocimiento en contexto.

Consecuentemente, la aplicación del concepto de entendimiento del JDP 2-00, en una misión de asesoramiento, pide que se preste mayor atención a los múltiples niveles de análisis y del ámbito mayor de comprensión espacio-temporal que permite que la opinión sea aplicada eficazmente.<sup>783</sup>

# Gestión de Inteligencia en las Américas

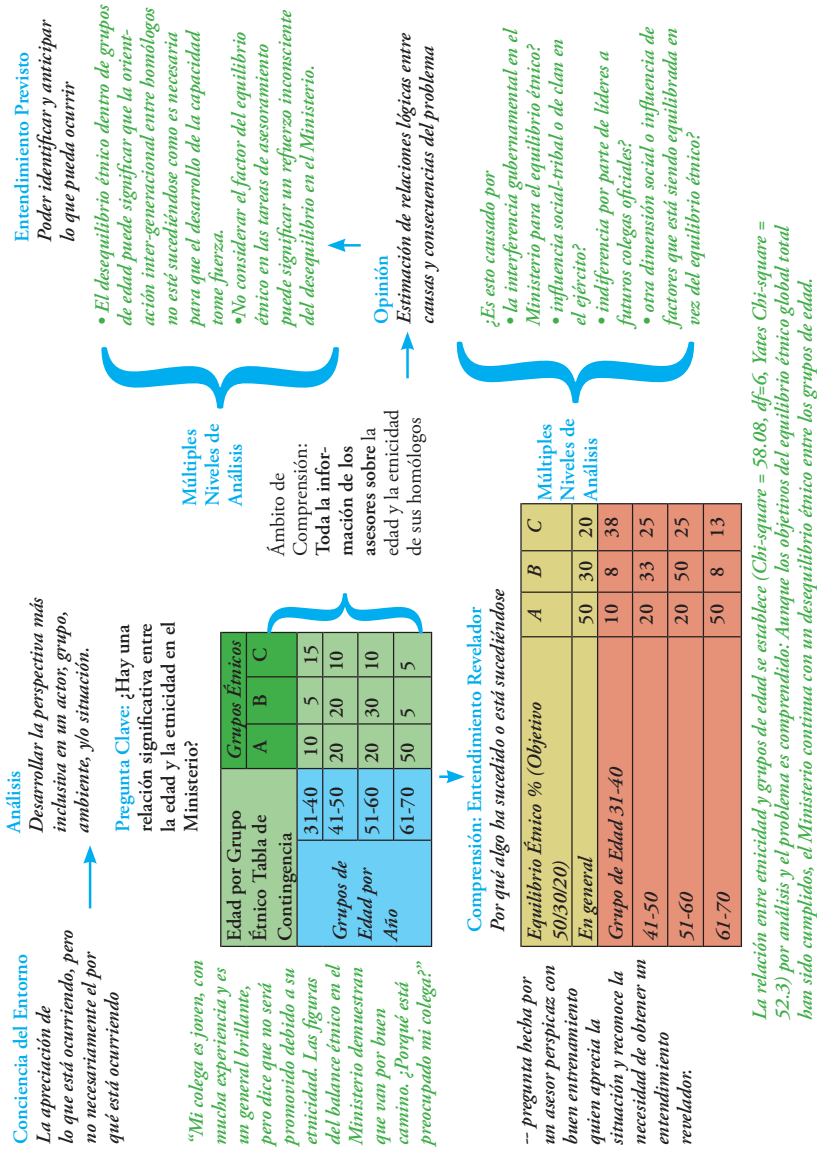


Figura 16. Reducir el Espacio entre la Conciencia del Entorno y el Entendimiento en un Problema Hipotético de reforma del Sector de Seguridad  
Fuente: Creado por los autores.

El diagrama muestra un ejemplo de progresión desde la conciencia de entorno inicial al entendimiento de las dinámicas socio-políticas, de relación y de comportamiento que afectan a una misión de asesoramiento ministerial.

En este ejemplo hipotético de un problema emergente de equilibrio étnico dentro del Ministerio de seguridad, los primeros cinco pasos para cerrar el espacio entre conciencia y entendimiento comienzan con un solo elemento de Conciencia del Entorno de un asesor bien entrenado. El homólogo del asesor hace una declaración que el asesor reconoce como insólito cuando las expectativas son que las políticas de equilibrio étnico están teniendo éxito. La preocupación del colega, dado sus calificaciones y edad, es reconocida por el asesor como un posible problema debido a la relación de la última con el contraparte y el conocimiento operativo de la planificación de la misión de asesoramiento y logros para el equilibrio étnico. El asesor, debido a la proximidad y relación con su colega, está también realizando una evaluación experta para averiguar si la preocupación del contraparte es por interés personal o falta de autoestima en el componente de equilibrio étnico de profesionalización y capacidad de construcción. Los analistas (de inteligencia) fuera de la misión de asesoramiento, que no tienen el conocimiento detallado y experto del asesor sobre la relación y de la misión operacional de asesoramiento, podrían no reconocer la declaración de la contraparte como un indicador de un posible problema sistémico de equilibrio étnico. Además, un analista externo típicamente permanece removido del ritmo rápido y ajustes veloces que son aspectos inevitables de una misión de asesoramiento de campo.

El segundo paso es el Análisis y esto requiere, como en todos los esfuerzos analíticos, identificar a la perspectiva más inclusiva de un actor, grupo, ambiente y/o situación para poder identificar correctamente la pregunta de investigación. En este ejemplo, el asesor reconoce la necesidad de entender si la contraparte está motivada solamente por ambición o por preocupaciones profesionales sobre los ideales de justicia y profesionalismo dentro de las políticas de equilibrio étnico. Responder a las preguntas del asesor requiere mucha más información que cualquier perspectiva deducida mediante una sola relación de asesoramiento. Para desarrollar la perspectiva necesariamente inclusiva, requiere un ámbito de comprensión que abarca las perspectivas de todos los asesores sobre las edades y etnicidades de sus homólogos.<sup>784</sup>

## Gestión de Inteligencia en las Américas

Eso es más fácil decirlo que hacerlo. Determinar la edad de las contrapartes no es tan directo como uno puede asumir. Muchas veces, las biografías oficiales no contienen esta información (aunque espacios para firmas -discutido anteriormente- puede y sí proveen pistas). El conocimiento detallado de patrones de avance en rangos en el antiguo ejército antes de la asistencia de fuerzas de seguridad, al igual que el conocimiento de eventos históricos -no siempre son conocidos y documentados en recursos disponibles en el Oeste- son útiles para estimar la edad si el asesor siente que sería inapropiado hacer preguntas para confirmarlo. Otra complicación es que la edad de la contraparte en archivos del ministerio, que en algunos países puede afectar el retiro y estado de la promoción, puede diferir de la edad verdadera y ser más importante. Una complicación final -y la más importante- es cómo identificar límites significantes para agrupar a los diferentes grupos de edades. Los militares crecen y cortan la fortaleza de sus tropas como un tema de competencia política doméstica del “control de armas” para fondos – como estamos viendo el hoy día en los Estados Unidos. A veces los militares tienen límites significantes para grupos de edades basados en eras de campañas militares – por ejemplo, en los EE.UU., las referencias a “Corea”, “Vietnam”, “Antes del 11/9”, “Después del 11/9” y otros muy cargados con experiencias personales, progresión en la carrera, y otros significados con énfasis doctrinal. Los ejércitos de otros países no son muy diferentes.

Es difícil para los asesores tratar de lidiar con esos temas sobre la edad de la contraparte, y aún más para los analistas fuera de la misión de asesoramiento. Esto es porque el ámbito de comprensión -conectar al desconectado y tomar el punto de vista histórico largo en un contexto de misión de asesoramiento- requiere acceso a todos los conocimientos de los asesores sobre todos los homólogos que los asesores quizás no pueden darse cuenta de lo que tienen. Los analistas externos, sin haber adquirido ellos mismos el entendimiento operacional de la misión de asesoramiento, no sabrán cómo ayudar a los asesores a lograr sus conocimientos. Un segundo problema yace en el análisis de la profundidad espacial-temporal, en que el conocimiento de historias nacionales, regionales, y de antes de la reforma del ejército publicadas localmente, al igual que entender cómo identificar a tribus y subgrupos étnicos y facciones (tales como de espacio de firma, como antes discutido) y la habilidad de leer el idioma de la contraparte, son importantes para asistir a un asesor a alcanzar y articular los conocimientos que tienen acerca



de sus homólogos. La profundidad del análisis -captar el conocimiento en contexto en este ejemplo de asesoramiento- será más estrecho y especializado. En este ejemplo hipotético, responder a la “pregunta de edad” incluirá el conocimiento experto sobre el personal del Ministerio, la promoción, y las políticas de mérito.

El tercer paso es la Comprensión, que produce un entendimiento extenso. La comprensión está estrechamente relacionada al análisis pero difiere de ésta en que la comparación adicional o manipulación de datos son realizadas para poder refinar el entendimiento del por qué algo ha sucedido o está sucediéndose. Considere las tablas en el diagrama anterior. En este ejemplo hipotético, la tabla de contingencia de Edad por Etnicidad fue producida al agregar la información de todos los asesores sobre la edad y etnicidad de sus colegas (y, cuando era necesario, realizar una investigación adicional para estimar la edad). Sin embargo, estos hallazgos no podrían fortalecer a los líderes de la misión de asesoramiento con el entendimiento extenso de cómo esto podría suceder, a pesar de cumplir con las sumas totales del porcentaje objetivo de equilibrio para los grupos étnicos. Para proveer esta perspectiva, las proporciones generales de equilibrio étnico necesitan ser comparadas con las proporciones de equilibrio étnico que fueron separadas por grupos de edad.

Llegar a la etapa de Comprensión en un contexto de asesoramiento ministerial muchas veces podrá requerir la captura del saber-cómo en un contexto sobre las funciones que están removidas de una preocupación de amenaza por parte de los analistas (de inteligencia) fuera de la misión de asesoramiento. En este ejemplo, la identificación y entendimiento del equilibrio étnico es ofuscado por sumas totales y entonces requiere saber y tener acceso a información sobre el personal del Ministerio, como la promoción, las políticas de mérito y los procedimientos. La fuente experta sobre este conocimiento e información será de hecho la misma misión de asesoramiento, *la cual hace con que los analistas externos sean más dependientes en la misión de asesoramiento en vez de que la misión de asesoramiento dependa de los analistas externos para producir comprensión.*

El entendimiento se logra con el cumplimiento de la Comprensión. Sin embargo, el entendimiento de perspectiva de la Comprensión es sobre el por qué algo existe o ha ocurrido. Para anticipar lo que puede pasar más allá del evento inicial, se requiere el cuarto paso, o sea la Decisión, por lo que significamos estimar las relaciones lógicas entre causa y consecuencia del problema.

## Gestión de Inteligencia en las Américas

Una misión de asesoramiento a nivel ministerial se compromete con una institución del sector de seguridad, la cual es una organización con dinámicas internas afectadas por dinámicas gubernamentales y de sociedad externas (ver Figura 15). La organización del ministerio de seguridad asesorada tendrá múltiples “constituyentes” ubicados dentro de múltiples niveles de la organización (soldados, comandos, comandos subordinados, sedes, etc.) del gobierno y la sociedad. Consecuentemente, una misión de reforma del sector de seguridad a nivel ministerial necesita múltiples niveles simultáneos de análisis para poder considerar todas las ubicaciones posibles donde las causas y consecuencias del problema pueden pasar. El cuarto paso es la Decisión, con su énfasis en múltiples niveles de análisis, la cual hace posible al Entendimiento Previsivo, el quinto y último paso para progresar de la conciencia del entorno al entendimiento. El Entendimiento Previsivo se refiere a ser capaz de identificar y anticipar lo que podría suceder, dado las relaciones lógicas identificadas entre causas y consecuencias del problema. Al igual que con la Decisión, el Entendimiento Previsivo depende de múltiples niveles de análisis. Sin embargo, los analistas fuera de la misión de asesoramiento pueden organizarse para enfocar su trabajo en un solo nivel (estratégico, operacional o táctico) en vez de múltiples niveles anidados. Esto podría llevar a un partidismo sistemático y resultar en omitir una clase de relaciones de causa-consecuencia posibles y futuros, resultados que pueden ser relevantes a la misión de asesoramiento.

### **Obstáculos adicionales legales y multinacionales en subcontratar la administración estratégica del capital intelectual de los asesores**

A estas alturas examinamos dos tipos generales de obstáculos que limitan la habilidad de organizaciones de inteligencia (tradicionales) de apoyar las necesidades de análisis socio-político de una misión de asesoramiento de la reforma del sector de seguridad a nivel ministerial. El primer tipo ocurre por la preocupación de comprometer a las relaciones de contrapartes, debido a la sospecha asociada con la interacción de asesores con el personal de inteligencia. Si parece haber consultas regulares con personal de inteligencia conocido, los asesores pueden correr el riesgo de que la misión de asesoramiento se convierta en ser, de hecho, los activos de recolección de inteligencia humana. También existe una preocupación generalizada de que la información intercambiada fuera de la misión de asesoramiento podría surgir en canales abiertos (Ej. *Wikileaks*).

El segundo tipo ocurre por las necesidades únicas de un asesor de nivel ministerial. Aun si las organizaciones de inteligencia pudieran legalmente apoyar a la misión de asesoramiento, los autores han discutido anteriormente cómo y por qué los asesores a nivel ministerial podrían ser los clientes más difíciles de complacer. El recurso de la organización de inteligencia y sus limitaciones de acceso al igual que el énfasis en la amenaza, limitan severamente sus habilidades de apoyar a los asesores a nivel ministerial. En Afganistán, los recursos de inteligencia militar a nivel operacional y de sede son limitados y se aplican juiciosamente sólo para apoyar al mandato de ISAF para la asistencia de seguridad en contrarrestar la insurgencia. Los requerimientos de prioridad de información (PIRs)<sup>785</sup> responden para involucrar una definición atada firmemente a la amenaza - dónde se ubica, qué tiene y qué es lo que puede hacer. Ya que el ANA-DEV estaba concentrado en construir capacidades en las fuerzas de seguridad afganas, y no preocupado con la amenaza de seguridad directamente, la inteligencia militar operacional no estaba en posición para tratar de las necesidades del ANA-DEV.

Los límites legales y multinacionales de la campaña, crean obstáculos adicionales para las organizaciones de inteligencia, apoyando a las necesidades socio-políticas de misiones de asesoramiento a nivel ministerial.

- Las advertencias únicas del manejo de información nacional y clasificaciones de inteligencia nacional obstaculizan acciones multinacionales y/o el intercambio de información. La simple existencia del Comando de Transición de Seguridad-Afganistán de los EE.UU. (CSTC-A), un elemento organizativo exclusivo a nivel nacional inicialmente separado de la Misión de Entrenamiento de la OTAN-Afganistán, opera fuera de la alianza para poder controlar las contribuciones nacionales y participación en la operación.<sup>786</sup> Con respecto a la clasificación de inteligencia, debido al ambiente ambiguo de seguridad de información multilateral, las políticas para clarificar los elementos de información que necesitan protección, no pudieron ser emitidas. El ISAF no tenía la autoridad de imponer una política de clasificación de seguridad coherente y unificada porque el ambiente multinacional incluía a voluntarios tanto nacionales como bilaterales de tropas contribuyentes aceptadas por GIROA que caían fuera del paraguas unificado de la OTAN.

## Gestión de Inteligencia en las Américas

- Algunos colegas afganos han pasado tiempo en los Estados Unidos, se han afiliados a corporaciones de los EE.UU. e inclusive se han casado con ciudadanos estadounidenses. Por lo tanto, estos afganos caen bajo la categoría de “Personas de EE.UU.” con protecciones legales contra recopilación de inteligencia estadounidense.
- La mayoría de los asesores contratistas en Afganistán están empleados bajo la Declaración de Trabajo (SOWs) que les impide de proporcionar información derivada de asesoramiento a organizaciones de inteligencia.
- Más críticamente, Afganistán es un aliado soberano y el mandato de NTM-A está sujeto a la renovación anual por el Consejo de Seguridad de las Naciones Unidas. La Comunidad de Inteligencia de los EE.UU. está legalmente restringida en cómo puede colaborar con el gobierno soberano de una nación aliada, y el ISAF tiene roles, autoridades y responsabilidades limitadas bajo los mandatos del Consejo de Seguridad de las Naciones Unidas.

En el dominio de asesoramiento, ANA-DEV era funcionalmente una Fuerza de Tareas tanto en su estructura y porque el Comandante tenía Requerimientos de Información Crítica (CCIRs). Dado el análisis único de información de la misión de asesoramiento, la administración de conocimiento y las necesidades de protección y preservación de la relación de asesoramiento, la mayoría de estos CCIRs no podría ser cumplidos fuera del ANA-DEV si todos los requerimientos legales de la Alianza debían sostenerse.

### Resolver el problema

El liderazgo del ANA-DEV estaba al tanto de la pérdida del capital intelectual del asesor al redespigar y se movió para detener esta pérdida de entendimiento e influencia. El comando de ANA-DEV aprobó una propuesta inicial permitiendo a los autores a trabajar en equipo para crear una capacidad interna que entrevistaría a asesores superiores para captar sus conocimientos y experiencias, desarrollar y refinar esta información con su contexto histórico y cultural, y luego educar a los sucesores de los asesores. Este equipo sirvió como una capacidad orgánica para captar, analizar, y mantener el capital intelectual de la misión al crear “continuidad mejorada” de los conocimientos e influencia de los asesores. Al cumplir con todas las cuatro características de la

administración estratégica del capital intelectual, esta capacidad interna facilitaría que la misión del asesor se convirtiera en una organización de aprendizaje. El equipo también tuvo la tarea de desarrollar los procedimientos operativos estándar para la administración, y retener y proteger la información del asesor de naturaleza sensible para una relación de asesoramiento. Este equipo de análisis e investigación con personal de asesores, realizarían deberes adicionales, incluyendo el desarrollo de estudios de facción y órdenes de batalla para el MoD y Personal General, creando proyectos de investigación de “únicas oportunidades” a pedido del asesor individual y del liderazgo al igual que iniciar una encuesta trimestral extensa y comprensiva del conocimiento de los asesores sobre las actitudes de sus homólogos en cuanto a proyectos e iniciativas de reforma del sector de seguridad.

El ANA-DEV no vio el tener capacidades de investigación y análisis orgánicos como no tener una invitación a participar en el campo de juego de la inteligencia. Lejos de eso, el ANA-DEV como una misión de asesoramiento, estaba preocupada principalmente con impedir cualquier posible amenaza para sus relaciones equivalentes. Una capacidad de investigación y análisis orgánica con personal compuesto por asesores bajo el control operativo de ANA-DEV y sin requerimientos de reportar a organizaciones familiares mitigaron todo el riesgo asociado con una misión de asesoramiento, tratando con inteligencia en un ambiente de Poder Inteligente con propósitos más allá de la protección por fuerza.

Para cumplir con las necesidades de ANA-DEV, los miembros del servicio necesitaban ser voluntarios altamente motivados dentro del ANA-DEV, que disfrutaban de buenos diálogos y la confianza de sus compañeros asesores. Ellos necesitaban tener un conocimiento profundo de la cultura, política, historia y el idioma afgano. Lo más importante es que los miembros del equipo necesitaban traer capacidades analíticas relevantes, conocimiento de métodos de las ciencias sociales, y experiencia en investigación aplicada para tener presente en el análisis y entendimiento los nuevos desarrollos de cada día.

El concepto requería que cada miembro desafiara la filosofía convencional, separaría hechos de opiniones y suposiciones, y continuamente persiguiera nueva información y conocimiento. Todos los miembros del equipo necesitaban tener el mismo grado de acceso a información oficialmente protegida, y tener mayor conocimiento sobre ésta y ser estrictamente observante de los códigos éticos relevantes y restricciones legales. Después de un mes de evaluación

## Gestión de Inteligencia en las Américas

de las mejores prácticas, de crear Procedimientos Estándar de Operación y protocolos de entrevista e instrumentos, y diseñar productos fundamentales que podrían ser actualizados regularmente, ANA-DEV estableció el primer equipo de Red Socio-Política y Análisis de Comportamiento (SNBAT).

El SNBAT fue establecido como un elemento dedicado y orgánico dentro del ANA-DEV y bajo el control directo del Comandante del ANA-DEV o su ayudante. El control directo incluyó el requerimiento de una autorización escrita por el Comandante del ANA-DEV para la distribución de cualquier producto de análisis. El Comandante necesitaba que el SNBAT fuese flexible y comunicativo con el CCIRS, el cual reflejaba el ambiente de asesoramiento dinámico y altamente fluido. El personal de SNBAT participaba activamente en las reuniones diarias de asesoramiento y conferencias del ANA-DEV, no sólo como asesores del MoD pero también para anticipar necesidades futuras y cambiantes de información. Ya que estas reuniones eran cerradas típicamente para todos salvo los asesores del ANA-DEV, la relación dedicada y orgánica era vital para la aprobación y cooperación de los asesores con el SNBAT.

Aunque el SNBAT del ANA-DEV fue el primer de su tipo para el asesoramiento ministerial, fue diseñado para aplicarse a los huecos de conocimiento basados en las mejores prácticas de esfuerzos anteriores. Mientras que el concepto de SNBAT está integrado en la necesidad de la misión de asesoramiento para un apoyo de análisis único, los autores encontraron los mejores modelos para balancear la flexibilidad y el control del comandante en cómo se organizaron los Equipos de Control de Análisis (ACTs), los “Equipos de Transición Militar Incrementados” (MiTTs) en Irak, y en los Equipos de Apoyo de Inteligencia de Compañía (CoISTs). El pequeño y enfocado ACT podía y sí brindó valor en Irak cuando los comandantes de la Brigada les dieron órdenes de enfocarse en donde la “niebla de la guerra” era un posible peligro para la operación. Los “MiTTs Incrementados” en Irak fueron capaces de completar espacios de información luego de recibir la autonomía de sus brigadas. Los CoISTs son otro ejemplo del uso de personal orgánico a la misión operativa para aplicarse a los huecos de conocimiento.

### *Dotación de personal para el ANA-DEV SNBAT*

El ANA-DEV inicialmente proporcionó personal para el equipo al capitalizar algunos de sus asesores de *Afganistán-Pakistán Hands* (APH). El programa

“Hands” de los Jefes de Estado Mayor de los EE.UU. ha desarrollado un cuadro de personal civil y militar con entendimiento de Darii o Pashto mediante cuatro meses de instrucción de inmersión de lenguaje, junto a la familiarización con “la cultura, la religión, la dinámica tribal, los estructuras y procesos del gobierno central y provincial, las estructuras y procesos de la seguridad afgana, entre otros temas de especialización.”<sup>788</sup> Luego, cuando un miembro del equipo fundador redesplegó, ese asiento fue ocupado por un Asesor del Ministerio de Defensa (MoDA). El programa de MoDA de la Agencia de Cooperación de Seguridad de Defensa de los EE.UU. “está diseñado para forjar relaciones a largo plazo que refuerzan al ministerio de defensa del estado socio. El programa combina a civiles superiores del Departamento de Defensa con requerimientos identificados de socios... Mientras desplegados, los asesores intercambian experiencia con sus homólogos en especialidades de defensa similares.”<sup>789</sup> El entrenamiento de MoDA incluye un curso extenso de siete semanas que cubre el entrenamiento del asesor, un conocimiento cultural de Afganistán y una familiarización con el país, al igual que instrucción en el idioma Darii.<sup>790</sup>

Proveer personal al SNBAT con asesores de “Hands” y del MoDA, hizo posible mantener al SNBAT bajo la autoridad del comandante de ANA-DEV. En teatro militar, “Hands” y MoDAs están puestos bajo el control operativo de los comandos a los cuales son asignados. El estatus de control operacional del equipo orgánico de SNBAT contribuyó a ganar la confianza y el apoyo de los asesores y líderes de Desarrollo de ANA, ya que ningún conflicto de intereses podría surgir con respecto a una necesidad de producir, compartir, o archivar productos o reportes para la promoción o el apoyo a otras cadenas de comando.

Una actividad clave del SNBAT era entrevistar a asesores del ANA-DEV para captar su conocimiento y beneficios de experiencia. Para ser completamente eficaz, además de captar el conocimiento socio-político, la entrevista tenía que ser un intercambio de experiencias e ideas que estimulaban al asesor invitado a recordar y compartir perspectivas valiosas, a compartir momentos de entendimiento y malentendidos entre culturas, y a pensar sobre nuevas técnicas de interacción que contribuyeron o pudieran mejorar el diálogo con su homólogo de la nación anfitriona. Para asegurar que las entrevistas captaran información en los dos sentidos, el personal del SNBAT tenía que ser hábil en conocimiento socio-político de Afganistán y en el asesoreamiento

## Gestión de Inteligencia en las Américas

ministerial y también ser capaz de poner a gusto a sus colegas durante las entrevistas.

### *Administración de información y manejo de datos del ANA-DEV*

La administración de información era una responsabilidad principal del SNBAT. Aunque los datos de los asesores no son típicamente relevantes en cuanto a amenazas, son altamente sensibles en relación al desarrollo de relaciones de asesoramiento. El equipo obtuvo todos los datos para asegurar la supervisión del comandante, y excedió los requerimientos establecidos de unidad inquilina de manera consistente con la obligación ética para maximizar la seguridad del asesor. El SNBAT consideraba a los asesores como siendo intrínsecamente “propietarios” de su información y los trataban como teniendo control de originador sobre su información y con ese control a ser “adquirido” por sus sucesores. Esto efectivamente puso a los asesores en control de hasta a qué punto su información sería utilizada en productos de SNBAT. Después que productos derivados fueran producidos, sólo el Comandante podría designar su distribución y empleo. El conocimiento funcional mutuo de los repositorios de información de teatro militar facilitó la distribución de lanzamiento de productos del SNBAT ordenado por el Comandante.

La administración de conocimiento del SNBAT requiere apreciación por la biblioteconomía. Los asesores generalmente intercambian libros y artículos útiles durante sus estadías. La oficina del SNBAT se convirtió en el sitio de la Biblioteca de Asesores, la cual los miembros del SNBAT expandieron con compras de libros publicados localmente, particularmente con libros de historia. Esta característica creció en importancia mientras el equipo aprendió más acerca de explicaciones de grupos étnicos de eventos históricos, algunos de los cuales variaban considerablemente con opiniones generales y explicaciones oficiales. También, entender las complejidades de la política afgana y la historia social entre los 60s y 70s fueron cruciales para entender los eventos formativos y las redes sociales forjadas durante las carreras iniciales de los homólogos afganos mayores del MoD.

### *Productos del ANA-DEV SNBAT*

El razonamiento principal detrás de la creación del SNBAT es mantener la continuidad de asesoramiento para mitigar la pérdida de las ventajas tácticas sociales, las perspectivas, y los conocimientos que el asesor saliente ha



desarrollado durante su año de asesoramiento. Para producir el primer Resumen de Continuidad de Asesoramiento, se requirió diseñar un instrumento de entrevista extenso en tanto ámbito y profundidad que (a) captaran el ámbito completo del conocimiento del asesor y relación con su homólogo y (b) capturaría la perspectiva del asesor en la relación con su homólogo dentro del MoD, dentro del GIROA, y dentro de la sociedad afgana.

El instrumento de entrevista era extenso, con más de 38 páginas de preguntas que típicamente tomaba entre 5 a 6 horas. La duración era necesaria para poder captar el alcance completo de la experiencia de asesoramiento del año. Los entrevistadores del SNBAT inicialmente pensaron que los asesores se resistirían y se rehusarían a sentarse para la entrevista debido a su duración. Sin embargo, después de algunas declinaciones iniciales, el SNBAT llegó a cumplir su meta de entrevistar exitosamente y completamente a la mayoría de los asesores superiores salientes después del primer mes de operación del equipo. Este logro se debió a la propagación por boca de que la entrevista, aunque larga, hizo un buen trabajo en captar las experiencias de los asesores a lo largo de su año de asesoramiento. Los autores también encontraron que los mensajes del SNBAT aliviaban las preocupaciones del asesor sobre ser juzgado. El SNBAT nunca sacó conclusiones sobre la relación de asesoramiento basándose en que cada relación de asesoramiento era única y porque el éxito de la relación de asesoramiento también está igualmente en las manos de su homólogo. Después del éxito del periodo de prueba inicial, el liderazgo del ANA-DEV hizo con que la entrevista de continuidad de asesoramiento fuese obligatoria para aquellos asesores que fueran desplegados nuevamente.

El instrumento de entrevista del SNBAT tenía cuatro secciones: la evaluación de su colega, la interacción de su homólogo con otros, la historia personal de su contraparte, y ubicación de la oficina, horario, y ritmo del homólogo. Dentro de cada sección había grupos de preguntas similares diseñadas para ayudar al asesor a recordar una variedad de subtemas.

Dos características adicionales del instrumento eran particularmente útiles: un inventario descriptivo de personalidad, y medios descriptivos para que un asesor pudiera identificar los niveles de habilidades cognitivas/aprendizaje de su colega. Estos brindaban a los asesores un léxico para describir a sus colegas. Los autores insertaron estas características porque la información de los rasgos de personalidad de sus homólogos y niveles de aprendizaje son muy

## Gestión de Inteligencia en las Américas

importantes para los asesores nuevos. Las respuestas de los asesores salientes a estas preguntas establecieron una base para que los futuros asesores pudieran tener una base de comparación si habían preocupaciones sobre el estado cognitivo y emocional de su colega.

El SNBAT también hizo uso de los análisis de redes sociales. Las misiones de asesoramiento crecen continuamente, cambian y entran en transición. Los colegas del ministerio de asesoramiento pueden ser recientemente designados, promovidos, retirados, y/o movidos lateralmente. Idealmente, los puntos de fricción y de falla deberían ser identificados antes de que la organización social se estrese para absorber e implementar un cambio institucional requerido por la organización de asesoramiento. Con una capacidad de análisis de red social, el comandante puede identificar relaciones que pueden facilitar u obstaculizar el esfuerzo de asesoramiento y facilitar o dificultar la capacidad de cambio dentro de la organización social.

Esta capacidad era la columna para un segundo producto acumulativo del SNBAT. El SNBAT produjo un “Orden de Batalla” distinguido por identificación y capas de facciones y grupos sociales informales dentro del Ministerio de Defensa y Personal General. El razonamiento detrás de este producto fue el reconocimiento que la influencia informal a veces importa al igual que la autoridad formal durante el periodo de flujo interino de la reforma del sector de seguridad cuando estándares profesionales aconsejados de la institución de seguridad están siendo identificados, codificados, y propagados. Los asesores estaban al tanto de estos diferentes tipos de poderes<sup>791</sup> y de cómo la influencia podría superar a la autoridad al detrimento de la profesionalización militar. El SNBAT extrajo conocimientos del grupo de asesores para identificar fuentes de grupo social y de facción de influencia mas allá de las amplias categorías de membresía étnica. Tanto el Resumen de Continuidad de Asesoramiento y el Orden de Batalla requerían varios meses de acumulación de capital intelectual antes de que comenzaran a brindar una vista panorámica de patrones y relaciones.

Una tercera iniciativa de producto del SNBAT fue una encuesta trimestral de asesores. Este producto fue diseñado para captar actitudes y opiniones indirectamente dentro del MoD sobre iniciativas de políticas de misión de asesoramiento y progreso hacia cumplir con esas iniciativas. El cuestionario de la encuesta trimestral era una mezcla de preguntas abiertas y cerradas que

investigaban las actitudes del MoD hacia los objetivos de la misión actual y permitía a los asesores notar las preocupaciones emergentes de sus homólogos. Esta encuesta variaba del resumen de Continuidad de Asesoramiento al concentrarse principalmente en lo contemporáneo (sólo con contenido histórico limitado) y por ser una total foto instantánea de actitudes en un tiempo relativamente corto. El liderazgo de ANA-DEV y sus asesores, de este modo, tuvieron su primer entendimiento extenso de actitudes y opiniones en el MoD sobre iniciativas actuales y preocupaciones emergentes analizadas desde un contexto de factores socio-políticos y de separaciones.

Con el paso del tiempo, el SNBAT comenzó a recibir pedidos de “estudios de una sola oportunidad”. El SNBAT respondió a pedidos de información por parte de los asesores sobre muchos temas variados, incluyendo la relación entre los géneros, el gobierno tradicional y la resolución de disputas, las facciones sociales, la sociedad civil, los aspectos sociales de salud y atención médica, la historia general, la organización social religiosa, y las diferencias en actitudes entre Kabul y otras áreas, entre otros.

### *El ciclo de vida del SNBAT y la aplicabilidad futura del concepto de SNBAT*

Las misiones de asesoramiento del sector de Seguridad no son permanentes. Todas las misiones de asesoramiento buscan, en las palabras del líder superior del NTM-A, “trabajar hasta quedarse sin trabajo”. Mientras los asesores trabajan para concluir su misión exitosamente, transiciones y cambios personales ocurrirán, incluyendo cambios a capacidades orgánicas tales como el SNBAT.

Cerca de finales del 2011, NTM-A reorganizó a algunos de sus comandos subordinados incluyendo el ANA-DEV, en vista de la nueva meta de una transición de las funciones de seguridad a ANSF en 2013. Unos meses después, el ANA-DEV como comando subordinado terminó su existencia separada y se fusionó con otro. El ANA-DEV SNBAT, por ser orgánico a ese comando, así dejó de operar. La declinación del ANA-DEV SNBAT fue natural y racional: como una capacidad orgánica y dedicada al comando, cuando ese comandose reorganizó o se eliminó, el SNBAT siguió esas mismas fortunas organizativas. Si el SNBAT hubiera continuado operando aparte de la misión de asesoramiento y bajo un razonamiento diferente de manejar el capital intelectual de esa misión, ésta se hubiera integrado al campo de inteligencia inapropiadamente.

## Gestión de Inteligencia en las Américas

Mientras el ANA-DEV declinaba, el ciclo de vida organizativo entero del ANA-DEV SNBAT pasó por una prueba de concepto de forma exitosa. Por haber hecho esto, el concepto del SNBAT en su ciclo de vida entero podrá ser aplicado a otras misiones de asesoramiento en el futuro.

Con ese propósito: ¿qué pueden aprender las futuras misiones de asesoramiento del ANA-DEV y de su SNBAT, fuera de la campaña de Afganistán de la OTAN, que desean preservar y usar el capital intelectual de sus asesores?

- Todas las misiones de asesoramiento del sector de seguridad son iniciativas del Poder Inteligente. El Poder Inteligente no sólo incrementa la necesidad de entendimiento socio-político, pero también el ámbito y los niveles de necesidad de entendimiento socio-político.
- El entendimiento socio-político del ambiente de asesoramiento no se trata de simplemente agregar las perspectivas del asesor individual; las perspectivas del asesor deben ser combinadas en una corporación coherente de capital intelectual.
- El capital no es producido por unos pocos asesores socio-políticos astutos; sino que el capital intelectual requiere las contribuciones de cada persona dentro de la organización de asesoramiento teniendo en cuenta las relaciones existentes.
- Las misiones de asesoramiento deben ser proactivas en la compilación, el análisis, la fusión y la retención del capital intelectual. Si las misiones de asesoramiento no hacen nada, los ciclos de reemplazo de asesores provocarán periodos de éxodos cíclicos del capital intelectual, que requieren una cantidad de tiempo considerable e interacción para reconstituirse - si es que pueden ser reconstruidos. Cuando las organizaciones son proactivas en mantener su capital intelectual, se convierten en organizaciones de aprendizaje.
- La administración estratégica del capital intelectual es una actividad organizativa orgánica e interna porque el capital intelectual es el componente crítico para convertirse en una organización de

aprendizaje. Una misión de asesoramiento que subcontrata su administración del capital intelectual fuera de las organizaciones, renuncia a convertirse en una organización de aprendizaje.

- La administración estratégica del capital intelectual de una misión de asesoramiento por una organización externa (especialmente por una organización de inteligencia) crea riesgos incluyendo el compromiso potencial de una relación de homólogos, vacilación por parte de los asesores a contribuir al capital intelectual, homólogos que pueden ser personas de los EE.UU. con protecciones legales contra la recolección de inteligencia de los EE.UU., y asuntos de soberanía.
- La administración estratégica del capital intelectual de una misión de asesoramiento por organizaciones externas está condenada al fracaso en el cumplimiento de las necesidades socio-políticas de la misión de asesoramiento. El entendimiento socio-político de la misión de asesoramiento yace en el análisis de políticas y conocimiento de las capacidades de construcción de la institución de seguridad. La fuente experta para estas entidades gemelas de conocimiento es la misma misión de asesoramiento, la cual hace que un analista externo sea más dependiente de la misión de asesoramiento con que la misión de asesoramiento sea dependiente del analista externo.
- Los miembros del SNBAT necesitan tener un dialogo fuerte con, y tener confianza en el cuerpo de asesoramiento. Todos los miembros del equipo deben tener el mismo grado de acceso a información oficialmente protegida e igualmente contribuir al análisis sin importar su posición en el equipo. Cada miembro del equipo debe tener conocimiento de la historia, la cultura, la política, y la sociedad de la nación anfitriona y tener destreza en un idioma. Además, los miembros del equipo deben traer diversas habilidades avanzadas al equipo y los miembros del equipo deben reconocer y respetar esas habilidades.
- Los miembros del equipo de SNBAT necesitan estar bajo el contr operativo del comandante de la misión y nadie más. El

## Gestión de Inteligencia en las Américas

control directo del comandante debe incluir el control sobre la distribución de cual quier producto de análisis.

- Los asesores mantienen control sobre su información, y ese control sería heredado por sus sucesores. El SNBAT retiene la información de los asesores para asegurar su entrega del asesor originario al asesor sucesor.

### **Conclusión: Los beneficios indirectos y residuales del SNBAT desde la perspectiva de un administrador de inteligencia**

A lo largo de este ensayo, los autores han analizado las necesidades del capital intelectual, los problemas, y la solución desde la perspectiva de los comandantes que lideran las misiones de asesoramiento en ambientes de Poder Inteligente complejos. La triada del aumento de necesidades de entendimiento socio-político, la discreción en el compromiso directo de la misión operacional con las naciones anfitrionas en asociaciones, y el manejo orgánico y estratégico del capital intelectual, no es único a las misiones de asesoramiento. Estas son necesidades para cualquier misión operacional asociada con la nación anfitriona y serán intensificadas en contextos de campañas multinacionales. Estas son consecuencias de desarrollo del Poder Inteligente y, al igual que la subida del Poder Inteligente, tiene consecuencias para el lado operacional de la reforma del sector de seguridad, también tendrá consecuencias para el lado de inteligencia.

Sin embargo, la explicación de los autores del por qué las actividades del SNBAT de una misión de asesoramiento deben permanecer aparte y separadas de las organizaciones de inteligencia tradicionales, no significa que las actividades del SNBAT existieron en oposición a las organizaciones de inteligencia u a otras misiones. La autonomía no es equivalente a la oposición, y los beneficios indirectos y residuales pueden acumularse en los servicios de inteligencia. Sin embargo, para que esto suceda, se requiere que la inteligencia se abstenga de ver las iniciativas del SNBAT como un recurso a ser absorbidos, incorporados y asignados. Esto no será un desafío, ya que existen paralelos en los cuales la Comunidad de Inteligencia de los EE.UU. ha beneficiado indirectamente y residualmente al mantener la autonomía e independencia de esfuerzos de investigación y análisis de campos fuera de la inteligencia.

Con el creciente valor que la Comunidad de Inteligencia pone en el análisis cultural,<sup>791</sup> se está volviendo difícil distinguir los productos analíticos de varias especializaciones de análisis de inteligencia de las publicaciones académicas o de la medida de asistencia de desarrollo y puntos de referencia de estudios de campo por parte del especialista de evaluación. Las aguas se vuelven aun más lodosas cuando uno considera que los productos de cada profesión incluyen protección de la información analizada, aunque en diferentes formas. El analista de inteligencia clasifica el producto dentro de un sistema que regula estrictamente quién tendrá acceso a ello. El académico está obligado legalmente y éticamente a proteger la identidad de sus fuentes de investigación colaboradoras bajo las leyes federales de los EE.UU. de protección del sujeto humano. El especialista de medidas de desarrollo y evaluación debe realizar su investigación bajo el principio de “no causar daño”. Por semejantes que sean los productos y los imperativos para proteger la información, los factores que determinan si las investigaciones y el análisis constituyen o no a un producto de inteligencia son la organización que la desarrolla y la audiencia o el cliente que la ha pedido. La Comunidad de Inteligencia se beneficia de los estudios académicos y de los de punto de referencia de desarrollo que están disponibles abiertamente y públicamente a todos. Los administradores de inteligencia reconocen que tratar de absorber, incorporar y asignar al académico universitario o al especialista en desarrollo organizacional extranjero podría poner en riesgo la habilidad de realizar investigaciones de aquellos individuos y de contribuir al conocimiento público desde el cual la Comunidad de Inteligencia también se beneficia.

Aunque los beneficios indirectos y residuales de la iniciativa del SNBAT son diferentes, buscar absorber, incorporar y asignar una misión operativa del SNBAT podría igualmente poner en riesgo la habilidad de realizar investigaciones y análisis para producir aquellos beneficios. ¿Cuáles son esos beneficios indirectos y residuales para la Comunidad de Inteligencia?

- El primer y principal beneficio es de menos pedidos de misiones de asesoramiento para información. La iniciativa de una misión de asesoramiento del SNBAT permite que la inteligencia se concentre en la amenaza (su fuerza tradicional). La capacidad del SNBAT hace esto al concentrarse en fortalecer directamente a los

## Gestión de Inteligencia en las Américas

asesores con conocimiento, no en construir una base de conocimiento que no podrán acceder directamente.

- Un segundo beneficio, particularmente para el creciente enfoque de la Comunidad de Inteligencia en el análisis cultural, es aumentar el número de gente con especializaciones en temas socio-políticos. El SNBAT fortalece a los asesores al incrementar el ámbito y amplitud de su conocimiento sobre las relaciones entre el ministerio de asesoramiento, el gobierno nacional y los gobiernos/comandos subnacionales. Mientras que los asesores son “correctores, no recopiladores”, estos conocimientos mejorados en tendencias individuales y de relaciones sociales, políticas y de comportamiento, están en una categoría de conocimiento fundamental comparable a conocimientos académicos publicados que los analistas de inteligencia encuentran útil y buscan.
- Un tercer beneficio se origina por parte de los esfuerzos de asesoramiento del sector de seguridad para construir las habilidades y las capacidades de inteligencia de la nación socia. Este esfuerzo requiere que el personal de asesoramiento sean individuos con experiencia en inteligencia quienes están y permanecen bajo el comando operacional de la misión de asesoramiento. El requerimiento de comando operacional, para la seguridad de la misión de asesoramiento, necesariamente suspende la relación de ese asesor con cualquier organización de inteligencia por la duración del despliegue. Sin embargo, los beneficios indirectos de las perspectivas de conocimiento base que dicho asesor puede ganar y regresar con él al volver a desplegar son muy diferentes a los que se acumulan por simplemente ser un “desplegado” como un activo de análisis de la organización. La mentoría verdadera y la construcción de relaciones (al contrario de sólo mantener contacto) permite que el individuo tenga acceso a ontologías sociales, políticas y culturales y conocimiento etnográfico. Esta es una inversión de capital humano inestimable en el analista y uno hecho posible por la administración estratégica de la misión de asesoramiento de su propio capital intelectual.



- Un cuarto beneficio resulta de la solución del SNBAT en proteger la información sensible del asesor. Los ambientes de Poder Inteligente Multilaterales producen organizaciones multinacionales que muchas veces avanzan antes de establecer políticas y guías de inteligencia unificadoras que operaciones de naciones individuales dan por sentado. Con el SNBAT, la información del asesor puede ser protegida de una divulgación no deseada sin tomar por defecto las soluciones inaplicables de una sola nación a una organización gobernada por mandatos internacionales.

Otros beneficios indirectos y residuales le ocurrirá sin duda al lector. Sin embargo, cualquiera de esos beneficios se acumulará sólo mediante la autonomía de la capacidad de la misión de asesoramiento del SNBAT.

Los autores han explicado cómo el ambiente de Poder Inteligente da forma a las misiones de asesoramiento, sus necesidades de entendimiento socio-político, y sus limitaciones en cumplir con esas necesidades. Mientras que el Poder Inteligente representa un paso evolucionario en la seguridad nacional de los EE.UU. y la política exterior, sus esfuerzos de inteligencia y sus operativos asociados también deben adoptarse. El ANA-DEV SNBAT es una ilustración de cómo los sucesores de los autores pueden adaptarse de forma organizativa a los ambientes de Poder Inteligente.

## Gestión de Inteligencia en las Américas

### Biografías de los autores

El **Coronel William S. Brei** asesoró al Ministerio de Defensa Afgano mientras servía en el programa *Afganistán-Pakistán Hands*. El fue el fundador y primer Jefe del ANA-DEV SNBAT. Durante despliegues anteriores, sirvió en la Base Aérea en 2002 y en 2005 como director del Aeropuerto Internacional Mazar-e Sharif. Se retiró de la Fuerza Aérea de los Estados Unidos en el 2012 después de una carrera de 28 años. WSBrei@yahoo.com

**Nathalie J. Frensley, Ph.D.** asesoró al Ministerio de Defensa Afgano mientras servía en el programa *Afganistán-Pakistán Hands*. Ella fue la fundadora y primera Directora de Investigación del SNBAT y la segunda Jefa del SNBAT. Anteriormente, ella fue una Científica Asociada de Investigaciones en el Instituto para Tecnología Avanzada, en la Universidad de Texas en Austin. Autor Correspondiente. NJFrensley@gmail.com.

El **Mayor Killaurin O. Roberts** asesoró al Ministerio de Defensa Afgano mientras servía en el programa *Afganistán-Pakistán Hands*. El fue el fundador y primer Suboficial de Asesoramiento del SNBAT. Anteriormente, el sirvió en la OTAN como Jefe de Fusión de Teatro del ISAF y de las Fuerzas de los EE.UU. como Mentor de Inteligencia Operativa durante los auges de Irak y Afganistán. Killaurin.Roberts@us.army.mil.



### Conclusiones

Carolina Sancho Hirane

El libro *Gestión de Inteligencia en las Américas*, constituye la tercera parte de una colección que comienza con el libro *Profesionalización de la Inteligencia* del 2004 y aborda el tema de la inteligencia gubernamental desde la perspectiva de quienes la concretan, los funcionarios que trabajan en los servicios y mira este tema desde la perspectiva de la profesionalización constatando los avances en la materia en diferentes países de la región americana. De esta manera, fue posible reconocer a los desafíos en cuanto a la formación y capacitación, que en ese período enfrentaban los servicios de inteligencia y el camino que habían seguido para llegar a ese estado.

Un segundo libro de la colección, fue presentado en 2009, titulado *Democratización de la función Inteligencia*, complementando la primera entrega al abordar el significado que ha tenido para los servicios de inteligencia en la región americana, el desempeñarse en el marco de sistemas políticos democráticos, junto con revisar el modo en que la cultura de inteligencia estratégica (del Estado) influyó en el tipo de inteligencia realizada en los diferentes países analizados en una perspectiva histórica y actual. De esta manera, se abordó el tema del contexto en el cual habían trabajado y trabajan los servicios de inteligencia de países de las américas hasta ese momento.

Este tercer libro, se adiciona a las anteriores entregas al abordar el tema del funcionamiento de los servicios de inteligencia hoy en la región americana, a partir de los desafíos que actualmente enfrentan al tener que desempeñarse en un contexto modificado por el fenómeno de la globalización. Dada la existencia de crecientes amenazas transnacionales a la seguridad, los países co-existen juntos, enfrentando a los desafíos nacionales propios de cada país que cada vez con mayor frecuencia presentan características similares en los diferentes Estados-nación de la región, con actores (estatales y no estatales) externos a los servicios de inteligencia cada vez más exigentes en cuanto a la eficiencia, eficacia, legalidad y transparencia en su funcionamiento. Igualmente, los servicios de inteligencia necesitan de recursos, capacidades, competencias y liderazgo acorde con los requerimientos, rol y misión que se les asigna, aun cuando se reconoce sin desconocer por ello la diversidad político, social, cultural, administrativa e histórica en esta zona geográfica. No

obstante, debido a la semejanza de los casos analizados en la zona indicada, nos permitimos desde la perspectiva de inteligencia hablar en términos genéricos de la “región americana”, sin desconocer por ello la variedad de realidades ella presenta.

La pregunta que ha orientado este esfuerzo académico ha sido, ¿cómo abordar estos desafíos diversos entre si y provenientes de distintos ámbitos y niveles de análisis?. La respuesta puede encontrarse a partir de cuatro ejes de análisis, presentados como secciones que dan cabida a varios artículos cada uno de los cuales presentan diferentes enfoques analíticos del tópico planteado. En efecto, los cuatro ejes a partir del cual se estructura el libro son: fiscalización de la inteligencia; gestión de la inteligencia desde el ejecutivo; gestión de la privacidad versus la seguridad y actuales desafíos de las comunidades de inteligencia y; gestión de la integración en inteligencia.

El primer eje, centrado en el marco legal bajo el cual funcionan los servicios de inteligencia, revisa la evolución de la regulación jurídica de diferentes países de la región americana hasta lo que existe actualmente, permitiéndonos constatar, que el control externo de los servicios de inteligencia en los países de las américas es en la mayor parte de éstos reciente y ha existido un proceso de aprendizaje a partir de escándalos y malas prácticas que han ocurrido en estos servicios públicos. Asimismo, la experticia en materia de fiscalización de servicios de inteligencia por parte del congreso o parlamento es reciente y su profundidad se ha conseguido por medio de la práctica en el desarrollo de esta actividad, no obstante se constata la necesidad de avanzar en este camino iniciado recientemente si lo comparamos con la fiscalización que estas mismas instituciones realiza a otras funciones públicas.

En esta perspectiva, uno de los puntos críticos en el control de los servicios de inteligencia está dado por el secreto, propio de la función inteligencia, clave para el desarrollo de su rol, tareas y misiones pero contrapuesto a uno de los principios del actuar público en sistemas políticos democráticos, observándose de este modo un dilema entre eficiencia en la gestión de un servicio público y legitimidad y transparencia de la función pública que desarrollan. Debido a que en esta ecuación está en juego la calidad misma de la democracia, como también, el apoyo que requiere para su gestión desde otros actores públicos, un adecuado control, que permita en espacios limitados y protegidos (por el compromiso del secreto de quienes accedan a esta información) dar cuenta

## Gestión de Inteligencia en las Américas

de las acciones desarrolladas, su metodología y los objetivos buscados resulta clave para promover dentro de los servicios de inteligencia, una gestión responsable que genere los estímulos correctos para el adecuado uso de la discrecionalidad entregada por el legislador. Poco a poco los países en las Américas progresan en este camino que en ocasiones presenta retrocesos y nuevos avances, permitiéndonos observar que por medio del ensayo y el error se construye una institucionalidad en la materia.

En efecto, uno de los principales aspectos críticos en el control de los servicios de inteligencia -la mayor discrecionalidad (que tienen en comparación con otros servicios públicos e inclusive entre los de seguridad) y el secreto- da fuerza a la importancia de promover y fortalecer la ética de cada uno de sus funcionarios. La dificultad de ejemplificar con casos verídicos la naturaleza y magnitud del problema, ha sido suplido por excelentes obras cinematográficas que permiten conocer en forma masiva la problematización de este asunto, facilitando la identificación de los dilemas a enfrentar y los valores que se contraponen (entre las más destacadas se encuentra libertad, seguridad, privacidad y respeto a los derechos humanos), dejando muchas veces abierto el debate y estimulando su discusión pública, privada e institucional, el cual sólo a través de la práctica ética de la función puede ofrecer respuestas concretas a las paradojas observadas.

En este sentido, el tema de la ética, emerge como una de las respuestas al problema, en sus distintos niveles de análisis y en los diferentes aspectos del funcionamiento de un servicio de inteligencia. Son variadas las formas en las cuales puede reforzarse a la ética en el trabajo de inteligencia, por ejemplo, por medio de códigos de ética, materia en la que existe escaso trabajo en la región. Sin embargo, junto a un adecuado y oportuno control externo puede colaborar en generar incentivos para el uso correcto de las atribuciones y competencias propias de los servicios de inteligencia, en particular esa mayor discrecionalidad y el secreto que poseen en comparación al resto de los servicios de la administración pública del Estado.

El segundo eje, centrado en la gestión de la inteligencia desde el poder Ejecutivo, aborda varias aristas en la materia. Una de ellas relacionada con el modo en que la función estatal de inteligencia se inserta en el proceso de toma de decisiones de las más altas autoridades políticas y las consecuencias que ello

produce en la relación productor – consumidor de inteligencia. También es revisada la manera en que es entendida la inteligencia estratégica, pues existe bastante prejuicio y confusión sobre el tema, sin embargo, hay algunos requisitos que éste debe cumplir para que sea considerada así, aun cuando se reconocen diferentes enfoques de la noción. Asimismo, al revisar los ámbitos de aplicación de la inteligencia en su nivel estratégico desde una perspectiva estatal contemporánea, se reconoce en el tema económico una dimensión que requiere mayor preocupación de los países americanos, pues siendo un factor clave en la estabilidad, crecimiento y desarrollo de los Estados, desde la perspectiva de la función estatal de inteligencia, se encuentra insuficientemente explorada y explotada.

Junto a lo anterior dos temas más son tratados. La relación entre inteligencia y presupuesto, relación muchas veces dejada de lado al tener poca capacidad los directivos de inteligencia de justificar adecuadamente sus necesidades económicas, afectando con ello en ocasiones, la obtención de recursos que condicionara el desarrollo de las tareas y misiones programadas. En este sentido, es necesario en inteligencia, contar con habilidades para dimensionar y explicar en forma clara y precisa los recursos que son necesarios para cumplir los requerimientos formulados desde el nivel político y que se traducen en tareas específicas para los servicios de inteligencia.

Finalmente, es tratado un aspecto frecuentemente polémico en los servicios de inteligencia, la cooperación en inteligencia, actividad inicialmente mirada con sospecha, por diferentes motivos entre los que destaca el miedo a vulnerar el secreto, dejar al descubierto vulnerabilidades, creer que las diferencias entre países y/o servicios son superiores a las similitudes, considerar que las materias en las cuales se compite impide relacionarse en aquellas donde hay intereses parecidos. Sin embargo, la creciente proliferación de amenazas transnacionales a la seguridad, como también, las declaraciones de los gobiernos de la región americana en instancias de encuentro multilaterales donde reconocen comunes amenazas a su seguridad, permiten mirar positivamente futuros progresos en cooperación en inteligencia en Suramérica. Esta afirmación se refuerza al constatar la experiencia que tiene cada uno de los países de esta zona geográfica en la función estatal de inteligencia (estratégica, militar y policial), como también su reconocida capacidad para cooperar en estos temas a nivel multilateral en cada uno de los ámbitos mencionados. En este sentido, queda

## Gestión de Inteligencia en las Américas

abierto el desafío para su realización en el marco de UNASUR, por medio de diferentes actividades que actualmente se desarrollan en otras instancias de cooperación, que sin embargo, pueden extrapolarse al organismo multilateral mencionado.

El tercer eje versa sobre la gestión de la tensión entre privacidad y seguridad, como también, sobre las comunidades de inteligencia y algunos de los desafíos que actualmente enfrentan. Respecto a la tensión entre seguridad y privacidad, cabe recordar que en principio la información de datos personales y sensibles de los ciudadanos son privados y en forma excepcional, transitoria y por justificados motivos cabe hacer una excepción al principio para acceder a información privada de los ciudadanos. En el marco del trabajo de los servicios de inteligencia, la mayor parte de éstos regulados por leyes de última generación, se ha establecido el procedimiento por medio del cual se accede a los datos de los individuos, previa autorización de una entidad externa a los servicios de inteligencia. Sin embargo, ello no siempre ha funcionado como se esperaba, es decir como un control que haga contrapeso a la capacidad (discrecionalidad) entregada a servicios de inteligencia de acceder a la información privada de los ciudadanos y que al acceder a ella no se haga mal uso de esta información.

En este sentido, las actuales tecnologías de la información y la comunicación (TIC) -junto al amplio uso de medios de comunicación social- facilitan para los servicios de inteligencia el acceso a gran cantidad de información dejando definitivamente en el pasado el problema del acceso a la información, dando paso a los desafíos del procesamiento de ésta, en términos de su valoración, clasificación y análisis principalmente. Por otro lado, quedan dudas respecto a la legitimidad de acceder a gran cantidad de información en forma masiva y sin límite de tiempo, contraviniendo en este sentido los clásicos principios que han guiado el acceso a información privada de los ciudadanos, que como se ha indicado corresponde a excepcionalidad, transitoriedad y justificación evidente (existencia de indicios y/o pruebas). Estamos ante una discusión pendiente que requiere consensos internacionales sobre esta práctica, pues el resultado del debate de este tema tendrá consecuencias para buena parte de las democracias que actualmente tienen servicios de inteligencia regulados por ley.



Desde una perspectiva nacional, la creciente necesidad de dar mayor especificidad al desarrollo de la función estatal de inteligencia, lleva al cuestionamiento del modo en que se integran los diferentes sistemas o comunidades nacionales de inteligencia. La necesidad de definir y formular estructuras de inteligencia criminal y penitenciaria, entre otras, obliga a revisar sus características propias, tales como sus similitudes y diferencias con aquellos organismos tradicionales de inteligencia (estratégico o gubernamental, policial, militar) y la relación que tendrán entre éstos. El modo como ha sido enfrentado el desafío en algunos países en América y Europa constituyen interesantes experiencias para analizar y evaluar la posibilidad de extrapolar a más países de la región americana a partir de la identificación de buenas prácticas y lecciones aprendidas.

Finalmente el tema de la cooperación y coordinación interagencial también requiere revisión desde una perspectiva de legislaciones nacionales y rendición de cuentas, con la finalidad de asegurar que éste se efectúe en los términos establecidos y para los fines autorizados, pues en ello se juega la legitimidad y legalidad de esta práctica, como también, su apoyo internacional y de la opinión pública.

El cuarto eje desarrollado en este libro, contempla el tema de la gestión de la integración en inteligencia, como un reto para los servicios de inteligencia. Su desarrollo contempla tres aristas. Una de ellas es la educación en inteligencia, como una política permanente que da respuesta a la necesidad de actualización y profundización de temas y materias por parte de los funcionarios de inteligencia, lo cual es responsabilidad de los servicios de inteligencia. El estímulo y monitoreo de una formación que promueva una permanente actualización y una continua integración de las capacidades de los servicios de inteligencia, debido a que los organismos de inteligencia no pueden darse el lujo de tener personas que trabajen en ellos y se encuentren desactualizados y cada vez más alejados del conocimiento y comprensión de todas las ramas del gobierno y sus órganos de recolección y análisis para entender un mundo cada vez más dinámico y complejo.

En esta perspectiva, existen diversos programas académicos de utilidad para funcionarios de inteligencia en el nivel estratégico, destacándose aquellos ofrecidos en el ámbito universitario, en contraposición a los que pueden ofrecer sus propias instituciones, pues éstos se justifican en actividades

## Gestión de Inteligencia en las Américas

secretas, pero no cuando son abordados temas generales que requieren una comprensión multidisciplinaria con énfasis en el debate y análisis crítico. Asimismo, se reconoce la existencia de programas académicos referidos a la función inteligencia en la región que han contribuido a dar un tratamiento especializado al tema a nivel de especialistas de la actividad, pero no en forma exclusiva ni excluyente.

La segunda arista es resultado de la TIC e ilustra cada una de las características del fenómeno de globalización, el cual condiciona el modo en que es realizada buena parte de las actividades cotidianas. Nos referimos al ciberespacio, descrita como la quinta dimensión de la guerra desde una perspectiva militar, que sin embargo, es mucho más que eso. Constituye el ambiente en el cual hoy las personas realizan cada vez más actividades diarias, desde comunicarse hasta efectuar transacciones bancarias y el desarrollo de una creciente cantidad de tareas laborales.

En este ambiente, resulta difícil distinguir las fronteras nacionales y las posibilidades de cooperación entre personas son ilimitadas, generando desafíos a la administración del ciberespacio o gestión de seguridad en ello, en términos de coordinación y creación de entidades a cargo de estas relaciones entre diversas organizaciones afines. La naturaleza de este ambiente da pleno sentido a nociones como “glocal” e “interméstico”, particularmente cuando se trata de evitar ataques o apropiación indebida de información. Pues una acción se puede realizar desde un lado opuesto del mundo donde se ubica el servidor afectado y puede tener consecuencias letales para un sistema y posiblemente la comunidad afectada que depende de éste (por ejemplo, en el caso de reactores nucleares). Asimismo, un ataque hacia una página web puede originarse en cualquier lugar del mundo y traerá consecuencias serias para los locales que requieran hacer uso de ella, ejemplo frecuente de esto, ocurre con los accesos a correos electrónicos de páginas institucionales e inclusive de bancos comerciales, en el sistema financiero.

Asimismo, el acceso a gran cantidad de información disponible, obliga a revisar el modo en que es posible acceder a esta información, las condiciones bajo las cuales se accede a ella y las características que debe tener este procedimiento. En este sentido, tanto la ciberseguridad en el ciberespacio, como el acceso a la información en éste para fines de inteligencia, plantea desafíos en

la forma en que tradicionalmente han sido entendidas ambas prácticas. Ello requiere un ajuste que considere un marco legal que lo regule y otorgue legitimidad política por medio de la oportuna disponibilidad de información a la opinión pública y un adecuado sistema de rendición de cuentas que garantice la inexistencia de abusos de parte de la autoridad autorizada a acceder a esta información.

La tercera arista considera la integración de información en un entorno común para los países que participan en misiones conjuntas multilaterales. En el caso de una misión de este tipo, como por ejemplo los Estados Unidos en Afganistán, vemos una construcción innovadora de recolección y análisis de campo, la cual reemplaza a la función tradicional de inteligencia. Este ejemplo innovador, de una gestión de información integrada, muestra cómo ésta puede ocupar un rol similar a la inteligencia misma, en un ámbito donde capacidades unilaterales de inteligencia no están bienvenidas, o de hecho son ilegales.

En síntesis, la gestión de la inteligencia en la región americana en sistemas políticos democráticos y en un contexto de globalización es una tarea compleja, debido a los diferentes temas que es necesario considerar en su funcionamiento, los diversos actores involucrados en ellos y la especificidad de las materias a tratar. Ninguna persona por si sola puede hacerlo y por ello el enfoque multidisciplinario resulta clave para una exitosa aproximación al tema. Este libro ha buscado ser un aporte en este sentido. Esperamos y confiamos en haber aportado en este camino.

## Gestión de Inteligencia en las Américas

### Notas de Fuentes Citadas

1 Russell G. Swenson y Susana C. Lemozy, coords., *Profesionalismo de Inteligencia en las Américas* (Washington, DC: Joint Military Intelligence College, 2004), disponible en [http://www.ni-u.edu/ni\\_press/pdf/Intelligence\\_Professionalism\\_in\\_the\\_Americas.pdf](http://www.ni-u.edu/ni_press/pdf/Intelligence_Professionalism_in_the_Americas.pdf).

2 Russell G. Swenson y Susana C. Lemozy, coords., *Democratización de la Función de Inteligencia: El Nexo de la Cultura Nacional y la Inteligencia Estratégica* (Washington, DC: National Defense Intelligence College, 2009), disponible en [http://www.ni-u.edu/ni\\_press/pdf/Democratización\\_de\\_la\\_Función\\_de\\_Inteligencia.pdf](http://www.ni-u.edu/ni_press/pdf/Democratización_de_la_Función_de_Inteligencia.pdf).

3 Guillermo Valdés Castellanos, Director, Centro de Investigación y Seguridad Nacional (CISEN) desde 2007 hasta 2011, en *CISEN: 20 Años de Historia—Testimonios* (México: CISEN, 2009), pp. 12-13. CISEN es la agencia de inteligencia civil de México.

4 Castellanos, *ibid*, p. 13.

5 Washington Platt, *Produção de Informações estratégicas*, trad. Mayor Álvaro Galvão Pereira y Capitão Heitor Aquino Ferreira (Rio de Janeiro: Biblioteca do Exército/Livraria Agir, 1974), p. 31.

6 Referirse a la breve descripción de SENSIPAM en la página principal del Sistema para la Protección del Amazonas (SIPAM) en <http://www.sipam.gov.br/>. Consultado 12 agosto 2012.

7 Referirse, por ejemplo, a la definición de “inteligencia nacional” en la Ley Pública de EE.UU. 108—458, Ley de Reforma de Inteligencia y Prevención de Terrorismo de 2004, sección 1012. Disponible en [http://www.nctc.gov/docs/pl108\\_458.pdf](http://www.nctc.gov/docs/pl108_458.pdf). Consultado 14 agosto 2012.

8 J. Edward Conway, “Analysis in Combat: the Deployed Threat Finance Analyst”, *Small Wars Journal* (julio 2012). Disponible en <http://smallwarsjournal.com/jrnll/artl/analysis-in-combat-the-deployed-threat-finance-analyst>. Consultado 30 julio 2012.

9 Referirse a la Federación de Científicos Americanos, Programa de Recursos de Inteligencia, en <http://www.fas.org/irp/world/index.html>.

10 Richard Helms, *A Look over My Shoulder: A Life in the Central Intelligence Agency* (New York: Random House, 2003), pp. 3-13.

11 Clifford Krauss, "Tapes Spy Chief Left Behind Scandalize Peru", *New York Times*, 3 febrero 2001. Disponible en <http://www.nytimes.com/2001/02/03/world/tapes-spy-chief-left-behind-scandalize-peru.html?pagewanted=all&src=pm>. Consultado 1 agosto 2012.

12 Florina Cristiana Matei y Thomas C. Bruneau, "Policymakers and Intelligence Reform in the New Democracies", y Maria do Céu Pinto, "Portugal's Intelligence Evolution in the Post-9-11 World", ambos en *International Journal of Intelligence and CounterIntelligence* 24, no. 4 (invierno 2011/2012), pp. 656-691, y 25, no. 1 (primavera 2012), pp. 160-177, respectivamente. Matei y Bruneau también cubren Polonia, Rumania y Rusia en su ensayo.

13 Gregory Weeks, "A Preference for Deference: Reforming the Military's Intelligence Role in Argentina, Chile and Peru", *Third World Quarterly* 29, no. 1 (2008), pp. 49-58. El autor determina que de estos tres países, sólo Argentina ha colocado actividades de inteligencia militar bajo supervisión civil.

14 Matei and Bruneau, *op. cit.*, p. 682.

15 Céu Pinto, *op. cit.*, pp. 165-167.

16 En los Estados Unidos, por ejemplo, la Orden Ejecutiva 12333 (1981), en su 2<sup>da</sup> parte, detalla las prohibiciones de actividades de recopilación. <http://www.archives.gov/federal-register/codification/executive-order/12333.html>. En adición, partes individuales de la Comunidad de Inteligencia pueden tener pautas adicionales. Por ejemplo, *Procedures Governing the Activities of Department of Defense Intelligence Components that Affect United States Persons, December 1982*, disponible en <http://latsdio.defense.gov/documents/52401-R.html>. Documento consultado 2 agosto 2012.

17 Corte de los Derechos Humanos Interamericanos, Demanda en el caso de Humberto Antonio Palamara Iribarne (Caso 11571) en contra de la República de Chile, 13 abril 2004.

18 Richard J. Aldrich, "Beyond the Vigilant State: Globalization and Intelligence", *Review of International Studies* 35 (2009), p. 900.

19 *Ibid*, p. 898. Para una apreciación de la importancia de información informal y la colaboración de inteligencia entre las fuerzas policiales, ver Michael D. Bayer, *The Blue Planet: Informal International Police Networks and National Intelligence* (Washington, DC: National Intelligence University Press, 2010). Disponible en [http://www.ni-u.edu/ni\\_press/pdf/The\\_Blue\\_Planet.pdf](http://www.ni-u.edu/ni_press/pdf/The_Blue_Planet.pdf).

## Gestión de Inteligencia en las Américas

20 Aldrich, *op. cit.*, p. 900.

21 Claudio Fuentes, “Political Dimensions of Security Transformation in Latin America”, *Institute of Development Studies Bulletin* 40, no. 2 (marzo 2009).

22 Por ejemplo, referirse a la fuente anónima de información de la Comunidad de Inteligencia para el libro de James Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York: Doubleday, 2008), p. 1.

23 Referirse a Gary Ross, *Who Watches the Watchmen?—The Conflict between National Security and Freedom of the Press* (Washington, DC: National Intelligence University Press, 2011). Disponible en [http://ni-u.edu/ni\\_press/pdf/Who\\_Watches\\_the\\_Watchmen.pdf](http://ni-u.edu/ni_press/pdf/Who_Watches_the_Watchmen.pdf). Consultado 11 agosto 2012.

24 Podemos tomar de ejemplos dos novelas interesantes: Jesús Emilio García Acosta, *El Ave del Pantano: Una Novela sobre la Inteligencia Estatal—el Segundo arte más antiguo de la humanidad y el primero de los dioses* (Bogotá: Editorial la Serpiente Emplumada, 2007) y Bravo León, *El Espía Francés: Crimen, Corrupción y Tráfico de armas en Chile* (Santiago: Origo Ediciones, 2011).

25 Referirse, por ejemplo, a los resultados de un estudio por el científico político Elizabeth A. Bloodgood, “What Do Decision-Makers Know?: The Sources and Evaluation of Information in Foreign Policy”, documento presentado originalmente en la reunión anual de la Asociación de Estudios Internacionales, febrero de 2003, en Portland, Oregón, disponible en [http://www.allacademic.com/meta/p\\_mla\\_apa\\_research\\_citation/0/6/4/5/6/pages64568/p64568-1.php](http://www.allacademic.com/meta/p_mla_apa_research_citation/0/6/4/5/6/pages64568/p64568-1.php). Consultado 12 agosto 2012.

26 Ohad Leslau, “The Effect of Intelligence on the Decisionmaking Process,” *International Journal of Intelligence and CounterIntelligence* 23, no. 3 (otoño 2010), pp. 426-448.

27 Stevyn D. Gibson, “Future Roles of the UK Intelligence System”, *Review of International Studies* 35 (2009), pp. 920-921.

28 *Ibid.*, p. 923.

29 Referirse a Richard J. Aldrich, *op. cit.*, pp. 891, 896-898. El autor señala en el día de hoy, debido a la estrecha relación existente entre la inteligencia y las operaciones, los “servicios secretos están haciendo menos análisis y prospectiva, y más ‘resolución, aplicación e interrupción’”. Bajo este punto de vista, la “rendición” de ciertas personas a la base de Guantánamo por parte de los servicios de inteligencia de los Estados Unidos fue más para derrumbar la estructura de Al Qaeda que extraerle información.

30 Robert M. Gates, “An Opportunity Unfulfilled: The Use and Perceptions of Intelligence at the White House”, *Washington Quarterly* 12, no. 1 (invierno de 1989): 35-44.

31 Richard K. Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (New York: Columbia University Press, 2007), p. 67. Todo el capítulo 4 está dedicado a este tema.

32 Nathan Woodard, “Tasting the Forbidden Fruit: Unlocking the Potential of Positive Politicization”, *Intelligence and National Security* 28, no. 1 (febrero 2013), pp. 91-108.

33 Josh Kerbel y Anthony Olcott, “The Intelligence-Policy Nexus: Synthesizing with Clients, not Analyzing for Customers”, *Studies in Intelligence* 54, no. 4 (diciembre de 2010), p. 5-7.

34 Referirse a una explicación del contexto para esta técnica en David T. Moore, *Sensemaking: A Structure for an Intelligence Revolution* (Washington, DC: National Intelligence University Press, 2011), pp. 64, 66.

35 En 2009, por ejemplo, el Director Nacional de Inteligencia de los EE.UU. declaró que “Una preocupación principal en el corto plazo para los Estados Unidos es la crisis económica global, junto con sus implicancias geopolíticas”. Véase Senate Select Committee on Intelligence, *Intelligence Community Annual Threat Assessment*, febrero 2009, p. 2. Disponible en <http://intelligence.senate.gov/090212/blair.pdf>. Consultado 30 Noviembre 2012.

36 Referirse a <http://www.egmontgroup.org/>. La relevancia de instituciones no gubernamentales en el ámbito de la inteligencia financiera está prevista en Gregory F. Treverton, “Intelligence and the Market State”, *Studies in Intelligence* 10 (invierno/primavera de 2001).

37 Cedric Chaffaut, “La unión europea, la geoeconomía y el patriotismo”, *Aainteligencia* (edición impresa) 1, no. 3 (marzo de 2008), pp. 50-53.

38 Este modelo informa el libro William J. Bernstein, *A Splendid Exchange: How Trade Shaped the World* (New York: Atlantic Monthly Press, 2008).

39 Russell G. Swenson y Susana C. Lemozy, *Democratización de la Función de Inteligencia: El Nexo de la Cultura Nacional y la Inteligencia Estratégica* (Washington, DC: National Defense Intelligence College, 2009), p. xxvi. Disponible en [www.ni-u.edu/ni\\_press/pdf/Democratización\\_de\\_la\\_Función\\_de\\_Inteligencia.pdf](http://www.ni-u.edu/ni_press/pdf/Democratización_de_la_Función_de_Inteligencia.pdf).

## Gestión de Inteligencia en las Américas

40 Referirse a Timothy Connors, “Putting the “L” into Intelligence-Led Policing: How Police Leaders Can Leverage *Intelligence Capability*,” *International Journal of Intelligence and CounterIntelligence* 22, no. 2 (verano de 2009), pp. 237-245. También Christopher Dickey, *Securing the City: Inside America’s Best Counterterrorism Force – the NYPD* (New York: Simon and Schuster, 2009).

41 Como bien documentado en Mark Riebling, *Wedge: The Secret War between the FBI and CIA* (New York: Alfred A. Knopf, 1994).

42 Richard K. Betts, *op. cit.*, p. 172.

43 Michael D. Bayer, *op. cit.*

44 *Ibid.*, pp. 109-111.

45 See Kevin Wirth, *The U.S. Coast Guard Programs Enters the Intelligence Community* (Washington, DC: National Defense Intelligence College, 2007), available at [http://www.ni-u.edu/ni\\_press/pdf/The\\_Coast\\_Guard\\_Intelligence\\_Program%20.pdf](http://www.ni-u.edu/ni_press/pdf/The_Coast_Guard_Intelligence_Program%20.pdf); Eric Ensign, *Intelligence in the Rum War at Sea, 1920-1933* (Joint Military Intelligence College, 2001), available at [http://ni-u.edu/ni\\_press/pdf/Intelligence\\_RUM\\_WAR.pdf](http://ni-u.edu/ni_press/pdf/Intelligence_RUM_WAR.pdf); and Martin Edwin Andersen, “A Roadmap for Beating Latin America’s Transnational Criminal Organizations,” *Joint Force Quarterly* 62 (julio de 2011), p. 86. Disponible en [www.ndu.edu/press/latin-america-transnational-criminal.html](http://www.ndu.edu/press/latin-america-transnational-criminal.html). Consultado 4 agosto 2012.

46 Como se menciona en el ensayo sobre policía e inteligencia en México (Swenson y Orozco), sección “El modelo de inteligencia policial para la supervisión y rendición de cuentas profesional”, y en James E. Steiner, “Improving Homeland Security at the State Level: Needed—State-Level Integrated Intelligence Enterprises”, *Studies in Intelligence* 53, no. 3 (octubre de 2009). Disponible en <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-53-no.-3/improving-homeland-security-at-the-state-level.html>. Consultado 10 agosto 2012.

47 Leslie A. Donovan, “Citizens as Intelligence Volunteers: The Impact of Value Structures”, *International Journal of Intelligence and CounterIntelligence* 18 (verano de 2005), p. 241.

48 Martin Edward Andersen, *op. cit.*

49 Mario Villarreal Díaz y Juan José Rico Urbiola, “La penalización de las actividades de inteligencia hostil en los órdenes subnacionales de gobierno en México: el caso ‘Nuevo León’”, en José Julio Fernández Rodríguez et al., *Cuestiones de*



*Inteligencia en la Sociedad Contemporánea* (Madrid: Ministerio de Defensa, Instituto Español de Estudios Estratégicos, 2011), pp. 175-185. Disponible en [http://www.portalcultura.mde.es/Galerias/publicaciones/fichero/Cuestiones\\_inteligencia.pdf](http://www.portalcultura.mde.es/Galerias/publicaciones/fichero/Cuestiones_inteligencia.pdf). Consultado 10 agosto 2012.

50 Para un ejemplo tomado de México, referirse a Efraín Medina Valenzuela, “La inteligencia como herramienta facilitadora del trabajo policial,” *AAInteligencia* (marzo de 2007). Disponible en <http://www.aaInteligencia.cl/?p=220>. Consultado 12 agosto 2012.

51 Mark Ungar, *Policing Democracy: Overcoming Obstacles to Citizen Security in Latin America* (Washington, DC: Woodrow Wilson Center Press, 2011), p. 67.

52 Mark Ungar, “The Privatization of Citizen Security in Latin America: From Elite Guards to Neighborhood Vigilantes,” *Social Justice* 34, nos. 3-4 (2007), p. 23.

53 Lucia Dammert, “La inseguridad urbana en Argentina: Diagnóstico y perspectivas”, pp. 283-315, en Fernando Carrión, ed., *Seguridad ciudadana, ¿espejismo o realidad?* (Quito: FLACSO Ecuador, 2002), pp. 301-307.

54 Referirse a Christopher Dickey, *op. cit.*

55 Jeff Stein, “NYPD Intelligence Detectives Go Their Own Way”, *Washington Post*, 10 noviembre 2010. Disponible en [http://voices.washingtonpost.com/spy-talk/2010/11/nypds\\_foreign\\_cops\\_play\\_outsid.html](http://voices.washingtonpost.com/spy-talk/2010/11/nypds_foreign_cops_play_outsid.html). Consultado 11 agosto 2012.

56 Mark Munson, “Assessing the New York Police Department’s Intelligence Efforts Targeting American Muslims”, *Small Wars Journal* (marzo de 2012). Disponible en <http://smallwarsjournal.com/jrn/art/assessing-the-new-york-police-department-s-intelligence-efforts-targeting-americas-muslims>. También referirse a *Small Wars Journal* Editors, “NYPD Intelligence Division: The Homegrown Threat”, *Small Wars Journal* (agosto de 2007). Disponible en <http://smallwarsjournal.com/blog/nypd-intelligence-division-the-homegrown-threat>. Ambos consultados 11 agosto 2012.

57 U.S. Department of Justice, *The Attorney General’s Guidelines for Domestic FBI Operations*, 29 septiembre 2008. Disponible en: <http://www.justice.gov/ag/reading-room/guidelines.pdf>. Consultado 11 agosto 2012.

58 El “Patriot Act” del 2001 (Public Law 107-56—Títulos VII, VIII and IX) de los Estados Unidos, vigente desde los ataques de 9/11, junto con el Intelligence Reform and Terrorism Prevention Act del 2004 (Public Law 108-458—Title 1, section 1016) son ejemplos. De modo similar, el presidente del Ecuador, Rafael

## Gestión de Inteligencia en las Américas

Correa, comenzó, en 2008, una revisión fundamental del sistema ecuatoriano de inteligencia aparentemente como resultado de su evaluación y renuncia de los métodos defectuosos de inteligencia ecuatoriana demostrados frente a la invasión colombiana en territorio nacional, donde se situaba una base de las FARC en el mes de marzo de ese año.

59 Russell G. Swenson, “Intelligence Education in the Americas,” *International Journal of Intelligence and CounterIntelligence* 16, no. 1 (Spring 2003): 108-130.

60 Véase, por ejemplo, la oportunidad mencionada en la página de la Escuela de Inteligencia del Ejército de Chile: <http://www.escint.cl/> (bajo “Curso Extranjeros”). Consultado el 11 September 2011.

61 Katitza Rodríguez, “The Politics of Surveillance: The Erosion of Privacy in Latin America”, Electronic Frontier Foundation, 22 Julio 2011. Disponible en <https://www.eff.org/deeplinks/2011/07/politics-surveillance-erosion-privacy-latin-america>. Consultado 11 agosto 2012.

62 Fernando Cocho Pérez, “Aprender la historia, comprender el entorno, saber para cambiar”, *Inteligencia y seguridad: Revista de análisis y prospectiva*, Madrid: N° 8 (junio-noviembre 2010). Luis Iberico es congresista peruana. El agregado es del autor.

63 “Control parlamentario de los servicios de inteligencia (...). Los Estados democráticos cuentan con diversos instrumentos y procedimientos para que el poder ejecutivo rinda cuentas sobre las actividades de los servicios de inteligencia ante el poder legislativo. (...). Las medidas adoptadas son propias y particulares de cada país y, generalmente, han aparecido vinculadas con el descubrimiento de casos concretos de funcionamiento irregular o de fracasos de sus servicios. Tampoco existe una doctrina general sobre el carácter y los límites del control a establecer, ya que se debe conciliar el imperativo de conocimiento y fiscalización de los servicios de inteligencia, por parte de los representantes de la nación, con la necesidad de preservar y proteger el secreto de la inteligencia producida y de las actividades realizadas, de los medios utilizados y de las fuentes de información usadas para su producción” [sic]. En: Miguel Ángel Esteban Navarro (coord.), *Glosario de Inteligencia* (Editado por la Secretaría General Técnica del Ministerio de Defensa de España, Imprenta Ministerio de Defensa de España, 2007), p. 66.

64 “Control judicial de los servicios de inteligencia (...). Normativa, procedimientos y órganos mediante los que el poder judicial vela por el respeto de la legalidad en general y de los derechos y libertades de los ciudadanos en particular por parte de los servicios de inteligencia durante el ejercicio de sus funciones. (...)” [sic]. *Ibid.*, p. 65.

65 “Control económico de los servicios de inteligencia (...). Normativa, procedimientos y órganos dispuestos para que los servicios de inteligencia rindan cuentas del uso de su presupuesto y los gastos en los que han incurrido durante el ejercicio de sus funciones. (...)”. [sic]. *Ibid.*, p. 65.

66 Diego Navarro Bonilla, *¡Espías! Tres mil años de información y secreto* (Madrid: Plaza & Valdez, 2009), p. 122.

67 Véase Fernando Rospigliosi, *Montesinos y las Fuerzas Armadas: Cómo controló durante una década las instituciones militares*, primera edición (Lima: IEP, diciembre 2000), pp. 70-73; Jorge Rodríguez Beruff, *Los militares y el poder—Un ensayo sobre la doctrina militar en el Perú: 1948-1968*, primera edición (Lima: Mosca Azul editores, 1983); Dirk Kruijt, *La Revolución por Decreto: El Perú durante el gobierno militar*, Serie Democracia y Fuerza Armada, N° 9 (Lima: IDL, 2008).

68 En ambas normas, del 27 de enero y del 30 de septiembre de 1960, se encuentra la firma del Presidente de la República, el refrendo de varios Ministros de Estado y el voto aprobatorio del Consejo de Ministros (en el considerando), con lo que las citadas normas cumplen y contienen los requisitos de forma.

69 El Decreto Supremo es: “una norma dada y aprobada por la más alta instancia del órgano ejecutivo, que es el Presidente de la República...”, en Marcial Rubio Correa, *El Sistema Jurídico: Introducción al Derecho*, sexta edición, corregida y aumentada (Lima: Fondo Editorial PUCP, 1993), p. 140. (Colección de textos jurídicos de la Pontificia Universidad Católica del Perú).

70 Víctor García Toma, *La Ley en el Perú: Técnica de elaboración, interpretación, aplicación e integración*, primera edición (Lima: Editorial Jurídica GRIJLEY, febrero 1995), p. 49.

71 Los acrónimos, de acuerdo con su secuencia de presentación, refieren a Secretaría de Inteligencia, Servicio Federal de Informaciones, Dirección Federal de Seguridad, Servicio de Inteligencia Colombiana, Departamento Administrativo de Seguridad, Dirección Nacional de los Servicios de Inteligencia y Prevención, Comité de Organización Política Electoral Independiente (un partido político).

72 Alejandro Valdivia Pedemonte, “¿Qué es un servicio de inteligencia?” *Revista de Marina* (noviembre-diciembre 1973—Lima: Marina de Guerra del Perú), pp. 626-629.

73 La ley N° 23720 fue promulgada el 13 de diciembre de 1983 y fue publicada al día siguiente de su promulgación.

## Gestión de Inteligencia en las Américas

74 Gustavo Gorriti, *Sendero: Historia de la guerra milenaria en el Perú* (Lima: Planeta, 2008).

75 Esta denominación ha sido creada por Andrés Gómez de la Torre sobre la base de lo señalado en: Dirk Kruijt y María del Pilar Tello, “De los reformistas militares a la Dictadura civil: La política militar peruana desde los años sesenta hasta el presente”, en Kees Koonings y Dirk Kruijt (eds.), *Ejércitos Políticos: Las Fuerzas Armadas y la Construcción de la Nación en la Era de la Democracia*, Serie: América Problema, 17, trad. Gabriela Ramos, primera edición (Lima: IEP, 2003), p. 97.

76 Anna Funder, *STASILAND: Historias del otro lado del Muro de Berlín* (Madrid: Tempus, 2009), p. 73.

77 Luis Piscocoya, “Inteligencia en el Perú: conceptos organizativos y manejo de crisis”, en, por varios autores, *Apuntes para una nueva visión de la Seguridad Nacional* (Lima: Instituto de Estudios Políticos y Estratégicos – IDEPE, 2004).

78 Véase Andrés Gómez de la Torre, “Del SIN al CNI y la DINI”, en Andrés Gómez de la Torre (comp.). *SIN Arcana Imperii: Inteligencia en democracia*, Primera edición (Lima: Foro Libertad & Seguridad, 2007), pp. 93-94.

79 J. Patrice McSherry, *Los Estados depredadores: la Operación Cóndor y la guerra encubierta en América Latina* (Santiago de Chile: LOM ediciones, 2009).

80 “Artículo 21º.- El Personal del Servicio de Inteligencia Nacional acreditará su condición de tal mediante un Carné de Identidad, que le facilitará el acceso a todas las reparticiones públicas y privadas, las mismas que, bajo responsabilidad penal, deberán obligatoriamente, permitir el acceso a sus instalaciones, y proporcionar la información y el apoyo requeridos para cumplimiento de las tareas encomendadas”, en Decreto Legislativo N° 746, *Ley del Sistema de Inteligencia Nacional*.

81 Este período de la inteligencia peruana resulta muy bien recreado en: Dirk Kruijt y María del Pilar Tello, *op. cit.*

82 Véanse: Fernando Rospigliosi, *Montesinos y las Fuerzas Armadas: Cómo controló durante una década las instituciones militares* (Lima: Instituto de Estudios Peruanos - IEP, 2000) y Carlos Iván Degregori, *La década de la antipolítica: Auge y huida de Alberto Fujimori y Vladimiro Montesinos* (Lima: IEP, 2001); también Jane Marcus-Delgado y Martín Tanaka, *Lecciones del final del fujimorismo*, Colección Mínima (Lima: IEP, 2001), p. 47.

83 Alberto Bolívar Ocampo, “Prefacio”, en Russell G. Swenson y Susana C. Lemozy (coords.) *Profesionalismo de inteligencia en las Américas*, edición revisada (Washington, DC: Joint Military Intelligence College, 2004), pp. 11-12. El agregado es del autor.

84 “Una *Ley Orgánica* es aquella que se requiere constitucionalmente para regular ciertas materias. Se oponen o distinguen de la ley ordinaria a nivel de competencias. Habitualmente para la aprobación de leyes orgánicas son necesarios requisitos extraordinarios como por ejemplo, mayoría absoluta o cualificada” [sic]. Disponible en [http://es.wikipedia.org/wiki/Ley\\_Org%C3%A1nica](http://es.wikipedia.org/wiki/Ley_Org%C3%A1nica). Consultado 19 abril 2012.

85 Andrés Gómez de la Torre, “Perú: Frustraciones en los intentos por reconstruir su sistema de inteligencia”, en Russell G. Swenson y Susana C. Lemozy (coords.), *op. cit.*, pp. 155-185.

86 La Defensoría del Pueblo del Perú es un ente gubernamental creado por la Constitución Política de 1993 para la protección de los derechos humanos en el país.

87 Defensoría del Pueblo, “La reforma y control de los servicios de inteligencia”, *Revista de la Defensoría del Pueblo, Debate Defensorial*, no. 3 (Mayo 2001), pp. 263-290. Disponible en [http://www.defensaydemocracia.org/uploads/2/0/5/7/2057202/defensoria-pueblo\\_reforma-control-servicios-inteligencia.pdf](http://www.defensaydemocracia.org/uploads/2/0/5/7/2057202/defensoria-pueblo_reforma-control-servicios-inteligencia.pdf). Consultado 13 marzo 2012.

88 Según la Real Academia de la Lengua Española, el secreto se define como: “Cosa que cuidadosamente se tiene reservada y oculta”, en: <http://www.rae.es/rae.html>. Consultado 8 febrero 2012.

89 “La única secrecía digna de confianza en cuestiones de Estado (...) es la que no solamente se impone el silencio, sino la que mantiene una reticencia juiciosa y considerada en asuntos en los que se percibe que el silencio es conveniente, aunque no se le haya impuesto. La fidelidad a los intereses públicos y a la confianza oficial y a la amistosa, exige un ejercicio cuidadoso de juicio sobre lo que se va a decir y lo que no, muchas veces cuando no se impone abiertamente el mandato de guardar el secreto (...)”, en <http://www.nexos.com.mx/?P=leerarticulo&Article=111976>. Consultado 8 febrero 2012.

90 Merece señalarse la extraordinaria y peligrosa similitud de los artículos 4º y 8º de la Ley N° 27479 del 2001, con los artículos 2º y 4º del Decreto Ley N° 25635 de 1992. Andrés Gómez de la Torre, “Evolución reciente y contextos de la legislación de inteligencia: El caso del Perú”, en Laura Chamorro (ed.), *Sistemas de Inteligencia comparados: Aportes al caso peruano*, primera edición (Lima: IDEPE, 2010), pp. 37-116.

91 Véase una obra precursora: José Manuel Ugarte, *Legislación de inteligencia: Legitimidad y eficacia* (Guatemala: Washington Office on Latin America y Asociación para el Estudio y Promoción de la Seguridad en Democracia, 2000). Ugarte junto con Jaime Garreta y Marcelo Fabián Saín fueron los impulsores y creadores de la Ley de Inteligencia nacional N° 25520 del 2001 en Argentina.

## Gestión de Inteligencia en las Américas

92 Ley N° 27479, *Ley del Sistema de Inteligencia Nacional (SINA)*, 11 junio 2001. “Artículo 36°— *Fiscalización*. Corresponde a la Comisión Ordinaria de Inteligencia del Congreso de la República fiscalizar el funcionamiento y ejecución de los recursos presupuestales del Consejo Nacional de Inteligencia, de conformidad con las normas constitucionales, Reglamento del Congreso y disposiciones legales vigentes”. *Disposiciones Transitorias*, “Quinta – La Comisión de Defensa Nacional, Orden Interno e Inteligencia del Congreso de la República asumirá las funciones de fiscalización hasta la creación de la Comisión Ordinaria de Inteligencia del Congreso”.

93 Un pre dictamen es una minuta o borrador del dictamen que se eleva a la Comisión Parlamentaria, luego dicho dictamen pasa al Pleno del Congreso, y si se aprueba pasa a ser autógrafa de Ley.

94 Ministerio de Justicia, Documento de Estudio 001-2004/JUS, *El servicio de inteligencia en un Estado de Derecho*, mayo 2004. Disponible en [http://www.defensaydemocracia.org/uploads/2/0/5/7/2057202/minjus\\_servintel-est-derecho.pdf](http://www.defensaydemocracia.org/uploads/2/0/5/7/2057202/minjus_servintel-est-derecho.pdf). Consultado 12 febrero 2012.

95 Véase: Resolución Suprema N° 097-2004-PCM, *Constituyen Comisión Especial encargada de implementar medidas aprobadas para la reestructuración del Consejo Nacional de Inteligencia*, publicada en el Diario Oficial *El Peruano*, 22 marzo 2004.

96 Perú, *Ley del Sistema de Inteligencia Nacional y de la Agencia de Inteligencia Estratégica*. Disponible en [http://www.idepe.org/pdf/proyecto\\_inteligencia.pdf](http://www.idepe.org/pdf/proyecto_inteligencia.pdf). Consultado 12 marzo 2012.

97 Referente a este tema, véase: Andrés Gómez de la Torre, “Comisiones reformadoras de inteligencia: Experiencias latinoamericanas recientes (2001-2009)”, en Fredy Rivera Vélez (coord.), *Inteligencia estratégica y prospectiva*, primera edición (Quito: FLACSO-SENAIN-AECID, mayo del 2011), pp. 185-186.

98 *Ley del Sistema de Inteligencia Nacional – SINA y de la Dirección Nacional de Inteligencia – DINI*, Ley N° 28664. Disponible en <http://www.congreso.gob.pe/ntley/Imagenes/Leyes/28664.pdf>. Consultado 10 marzo 2012.

99 “Operaciones especiales. Acciones operativas de inteligencia y contrainteligencia, que suponen la transgresión de determinados derechos ciudadanos, en razón de amenazas a la seguridad nacional, requiriendo previa autorización judicial para su realización” [sic], en *Ley del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia – DINI*, Ley N° 28664, Primera Disposición Complementaria, Glosario.

100 Ley N° 28664. Disponible en <http://www.congreso.gob.pe/ntley/Imagenes/Leyes/28664.pdf>. Consultado 6 marzo 2012. La UIF-PERÚ es miembro de *The Egmont Group of Financial Intelligence Units*, “El objetivo del Grupo Egmont es proporcionar un foro para las UIF de todo el mundo para mejorar la cooperación en la lucha contra el lavado de dinero y financiación del terrorismo y de fomentar la aplicación de los programas nacionales en este campo”. Disponible en <http://www.egmontgroup.org/>. Consultado 6 marzo 2012.

101 Mediante Ley N° 29038, la Unidad de Inteligencia Financiera del Perú (UIF-PERÚ) fue incorporada a la Superintendencia de Banca, Seguros, y Administradoras Privadas de Fondos de Pensiones (SBS).

102 Un miembro accesorio es un término parlamentario peruano, cuyo sinónimo es “suplente”.

103 Referente al caso “*MARTE-DINTEMAR*” de la venta de información de inteligencia. Disponible en <http://www.desdeeltercer piso.com/cat/carlos-barba/>. Consultado 09 marzo 2012; referente al caso “*BTR*” véase url: <http://www.larepublica.pe/06-10-2011/caso-btr-gustavo-gorriti-cuenta-la-historia-de-los-correos-truchos>. Consultado 9 marzo 2012.

104 Véanse el Capítulo II del Título II de la Ley N° 28664, especialmente los artículos 14°, 15° y 16°; y el Capítulo III del Título II, especialmente los artículos 20° y 21°.

105 Véanse los artículos 3° y 5° de la Ley N° 28664.

106 Este Grupo de Trabajo se crea en concordancia con el Reglamento del Congreso, que tiene fuerza de ley y regula las actividades y funcionamiento de las Comisiones Ordinarias Parlamentarias.

107 El citado informe se encuentra en los archivos del Congreso de la República del Perú.

108 Según el *Manual de Inteligencia Estratégica del SINA*, las Notas de Información deben ser formuladas “(...) en forma clara, precisa y concisa, dando respuesta a las principales interrogantes: qué o quién, cuándo, dónde, cómo y por qué o para qué” [sic], y las Notas de Inteligencia son el paso final del Procesamiento de las Informaciones. Véase en: *Manual de Inteligencia Estratégica del SINA*, Tomo I, Escuela de Inteligencia Nacional – ESIN, 1994, pp. 56 y 74.

## Gestión de Inteligencia en las Américas

109 Proyecto de Ley N° 2563-2007-CR, *Proyecto de Ley que modifica la Ley N° 28664, Ley del Sistema de Inteligencia Nacional – SINA y de la Dirección Nacional de Inteligencia – DINA*. Disponible en <http://www2.congreso.gob.pe/Sicr/TraDocEstProcl/CLProLey2006.nsf>. Consultado 6 marzo 2012.

110 Referente al control judicial, véase: Brasil, *Ley N° 9883*, art. 3° Parágrafo Único; Argentina: *Ley N° 25.520*, Título VI, art. 18° al 22°; Chile: *Ley N° 19.974*, Título V, art. 23° al 32°. Y, referente al control parlamentario, véase: Brasil: *Ley N° 9883*, art. 6°; Argentina: *Ley N° 25.520*, Título VIII, art. 31° al 41°; Chile: *Ley N° 19.974*, Título VI, art. 33° al 37°.

111 Referente a la transparencia en información de inteligencia véanse los artículos acerca de la captura de “Artemio” Gustavo Gorriti, “Crepúsculo en la madrugada”, revista *Caretas*. Disponible en <http://www.caretas.com.pe/Main.asp?T=3082&S=&id=12&idE=1000&idSTo=0&idA=57237&NL=1>. Y, “Cazando a ‘Artemio’”, revista *Caretas*. Disponible en <http://www.caretas.com.pe/Main.asp?T=3082&S=&id=12&idE=1000&idSTo=0&idA=57238>. Consultados 9 marzo 2012.

112 Referente al tema, véase el trabajo precursor en: José Manuel Ugarte, “El control de la actividad de Inteligencia: Realidad actual y tendencias hacia el futuro – Un análisis centrado en América Latina”, presentado en Santiago de Chile, Center for Hemispheric Defense Studies, REDES 2003; así también, véase: Andrés Gómez de la Torre, “Servicios de Inteligencia y democracia en América del Sur. ¿Hacia una segunda generación de reformas normativas?”, *Agenda Internacional* (Instituto de Estudios Internacionales, IDEI-PUC), Año XVI, N° 27, 2009, pp. 119-130.

113 *Decreto Ley N° 9*, del 20 de agosto del 2009. Disponible en [http://www.gacetaoficial.gob.pa/pdfTemp/26109/GacetaNo\\_26109\\_20080822.pdf](http://www.gacetaoficial.gob.pa/pdfTemp/26109/GacetaNo_26109_20080822.pdf). Consultado 12 marzo 2012.

114 Véase *Proyecto de Ley N° 026*, del 12 de agosto del 2009. Disponible en [http://www.asamblea.gob.pa/apps/seg\\_legis/PDF\\_SEG/PDF\\_SEG\\_2000/PDF\\_SEG\\_2009/2009\\_P\\_026.pdf](http://www.asamblea.gob.pa/apps/seg_legis/PDF_SEG/PDF_SEG_2000/PDF_SEG_2009/2009_P_026.pdf). Consultado 12 marzo 2012.

115 El 5 de marzo del 2010, la Comisión Colombiana de Juristas (CCJ) y la Corporación Reiniciar presentaron una demanda de inconstitucionalidad por una serie de vicios de forma en la tramitación, y también por vicios de fondo en los que incurrieron varios artículos de la citada ley. El texto de la síntesis de la demanda de inconstitucionalidad de la ley de inteligencia y contrainteligencia se encuentra disponible en <http://www.coljuristas.org/Portals/0/IS%C3%ADntesisinteligencia.pdf>. Consultado 29 noviembre 2010.



116 Para un comentario del caso colombiano referente a espionaje y la declaración de inconstitucionalidad de la Ley de Inteligencia y Contrainteligencia por la Corte Constitucional, también véase: Alejo Vargas Velásquez, “La Inteligencia está de moda”, *El Colombiano.com* [En línea] (2010). Disponible en [http://www.elcolombiano.com/BancoConocimiento/L/la\\_inteligencia\\_esta\\_de\\_moda/la\\_inteligencia\\_esta\\_de\\_moda.asp](http://www.elcolombiano.com/BancoConocimiento/L/la_inteligencia_esta_de_moda/la_inteligencia_esta_de_moda.asp). Consultado 2 Diciembre 2010.

117 Andrés Gómez de la Torre y Raúl Santiago Calle Peña, *Inteligencia en los Andes: Avances y retrocesos* (Centro Andino de Estudios Estratégicos - CENAE), julio 2011, p. 6. También disponible en <http://www.resdal.org/producciones-miembros/inteligencia-en-los-andes2.pdf>. Consultado 12 marzo 2012.

118 Véase “Agencia que reemplaza al DAS no será policial,” en <http://www.elpais.com.co/elpais/colombia/noticias/agencia-reemplaza-das-sera-policial>. Consultado 10 febrero 2012.

119 “Dirección Nacional de Inteligencia tendrá un Inspector General que vigilará el cumplimiento de la ley”, véase en [http://wsp.presidencia.gov.co/Prensa/2011/Noviembre/Paginas/20111104\\_15.aspx](http://wsp.presidencia.gov.co/Prensa/2011/Noviembre/Paginas/20111104_15.aspx). Consultado 9 marzo 2012.

120 “Angostura marcó un antes y un después en las FFAA”. Disponible en <http://www.hoy.com.ec/noticias-ecuador/angostura-marco-un-antes-y-un-despues-en-las-ffaa-328808.html>. Consultado 9 marzo 2012.

121 Estos principios se encuentran contemplados en el citado Proyecto de Ley: “Artículo 4º.- En la recolección y tratamiento de la información, las autoridades de inteligencia deberán ajustar su actuación a los siguientes principios: *Legitimidad* (sometimiento pleno a la ley, derecho y actuación de acuerdo a la subordinación y responsabilidad orgánicas). *Eficiencia* (adecuada relación entre los medios puestos a disposición y la calidad y oportunidad del producto obtenido – la inteligencia). *Financiamiento* (origen y aplicación adecuados de los fondos asignados a los servicios, incluso los reservados). La estricta observancia de la *legalidad* de aquellos procedimientos que, inevitablemente, requieran de actividades invasivas de la privacidad de los individuos. La estricta observancia de los principios de *necesidad y diseminación*. Se requerirá la información necesaria para la correcta y cabal ejecución de las funciones en cada una de las áreas anteriormente definidas, y se resguardará para tales fines. Asegurar que la información no sea empleada en beneficio específico de persona, organización privada o partido político alguno” [sic].

122 Decreto N° 6067 (derogado), con Rango, Valor y Fuerza de Ley, del Sistema Nacional de Inteligencia y Contrainteligencia, *Gaceta Oficial de la República Bolivariana de Venezuela* N° 38940, 28 mayo 2008.

## Gestión de Inteligencia en las Américas

123 Referente al SEBIN, véase <http://www.intelpage.info/servicio-bolivariano-de-inteligencia-nacional-sebin.html>. Consultado 9 marzo 2012.

124 Para mayores alcances, véase: Andrés Gómez de la Torre Rotta, “Comisiones reformadoras de Inteligencia: experiencias latinoamericanas recientes (2001-2009)”, en Fredy Rivera Vélez, *op. cit.*, pp. 190-191.

125 Esta evolución u “*hoja de ruta*” surgió a partir de los siguientes pasos: “a) Escándalo; b) Constitución y establecimiento de una comisión evaluadora / investigadora; c) Informe final de la comisión que incluye conclusiones y recomendaciones, entre ellas la necesidad de un nuevo marco normativo para fortalecer el sector; d) Proyecto de ley, generalmente preparado por el poder ejecutivo (Ecuador, Costa Rica) y / o con aportes de otros proyectos de ley generados desde el congreso (Perú, Colombia); y, e) Nuevo marco normativo con énfasis en leyes de inteligencia que incluyan mecanismos de contrapeso político frente al sistema de inteligencia y controles democráticos desde el congreso (control externo) y judicial (control paralelo)”, citado en: Andrés Gómez de la Torre Rotta. “Servicios de Inteligencia”, *op. cit.*, p. 127. También véase: Andrés Gómez de la Torre Rotta, “Comisiones reformadoras”, *op. cit.*, pp. 179-180.

126 Este tema se encuentra desarrollado en, Andrés Gómez de la Torre Rotta, “Comisiones reformadoras”, *op. cit.*, pp. 177-196.

127 “El control social, probablemente el más importante de todos, pues se trata del escrutinio independiente que pueden ejercer la prensa, los partidos políticos, la opinión pública, los académicos y los centros de estudio”, citado en, Carlos Maldonado, “Desafíos de los servicios de inteligencia en la región andina”, en Andrés Gómez de la Torre (comp.), *SIN Arcana Imperii: Inteligencia en democracia* (Lima: Foro Libertad & Seguridad, abril del 2007), p. 273.

128 Véase José Julio Fernández Rodríguez y Daniel Sansó-Rubert Pascual, “El recurso constitucional a las fuerzas armadas para el mantenimiento de la seguridad interior: el caso de Iberoamérica”, *Boletín Mexicano de Derecho Comparado*, XLIII, N° 128 (México: Instituto de Investigaciones Jurídicas-UNAM, mayo-agosto 2010), pp. 737-760. Así también véase Kate Martin, “Domestic Intelligence and Civil Liberties”, *SAIS Review*, XXIV, N° 1 (invierno-primavera 2004), pp. 7-21. En el caso peruano el Proyecto de Ley N° 1374/2006-PE y el Dictamen N° 17 del citado proyecto, permitieron la dación de la Ley N° 29166, denominada *Ley que establece reglas de empleo de la fuerza por parte del personal de las fuerzas armadas en el territorio nacional*, donde se establece la tendencia legislativa peruana de habilitar a las fuerzas armadas en tareas de orden interno o apoyo en el restablecimiento del

mismo. Disponible en <http://www.congreso.gob.pe/ntley/Imágenes/Leyes/29166.pdf>. Consultado 13 marzo 2012.

129 La Ley 29915 delegó al poder ejecutivo la oportunidad de legislar, durante un periodo de 90 días, sobre “Reforma del sistema de seguridad y defensa nacional con el objeto de fortalecer su constitución y funcionamiento”. Véase [http://www.mef.gob.pe/contenidos/servicios\\_web/conectamef/pdf/normas\\_legales\\_2012/NL20120912.PDF](http://www.mef.gob.pe/contenidos/servicios_web/conectamef/pdf/normas_legales_2012/NL20120912.PDF).

130 Se trata de los Proyectos de Ley 721/2012-CR, 722/2012-CR, 724/2012-CR, 728/2012-CR y 730/2012-CR.

131 Véase el texto completo del Decreto en <http://dataonline.gacetajuridica.com.pe/gaceta/admin/elperuano/2012-11-12/11-12-2012.PDF>.

132 Teóricamente, el congreso peruano podría declarar no constitucional el Decreto Legislativo 1141, aunque parece improbable que lo hagan. En todo caso, el proceso de redacción e implementación del decreto queda en manos de la rama ejecutiva.

133 José Manuel Ugarte, “Controle público da atividade de inteligência: a procura de legitimidade e eficácia”, em Brasil, Congresso Nacional, *Anais do Seminário Atividades de Inteligência no Brasil: Contribuições para a Soberania e a Democracia, de 6 a 7 de novembro de 2002* (Brasília: Agência brasileira de inteligência-Abin, 2003), pp. 89-145.

134 Thomas Bruneau, “*Intelligence and Democratization: The Challenge of Control in New Democracies*”, The Center for Civil-Military Relations – Naval Postgraduate School, Monterey California – Occasional Paper # 5 (março 2000).

135 Peter Gill, *Policing Politics: Security Intelligence and the Liberal Democratic State* (London: Frank Cass, 1994).

136 O vocábulo “inteligência” foi incorporado à doutrina brasileira a partir da década de 1990, após a redemocratização, substituindo a terminologia “informações”, mais adequada à língua portuguesa. As razões dessa mudança foram, sobretudo, de ordem política, de modo a se tentar banir termos associados ao regime militar – como também aconteceu com a expressão “segurança nacional”. Fica o esclarecimento de que, atualmente no Brasil, “informações” é entendido como “inteligência”, que também não é a mesma coisa de “informação”, esta última mais relacionada com um conjunto de conhecimentos reunidos sobre determinado assunto. A esse respeito vide, de nossa autoria, *Atividade de Inteligência e Legislação Correlata*, segunda edição (Niterói: Impetus, 2011).

## Gestão de Inteligência em las Américas

137 Apesar de alguns autores que escrevem sobre atividade de inteligência no Brasil falarem de “ações encobertas” e “ações clandestinas”, esses termos são completamente alheios à doutrina brasileira de inteligência, não sendo usados pelos profissionais da área no País. No Brasil, fala-se de “operações de inteligência”; o restante constitui terminologia alienígena e sem qualquer emprego pelos brasileiros.

138 Ainda na Antigüidade, em sua obra clássica sobre estratégia, *A Arte da Guerra*, o general chinês Sun Tzu (século IV a.C.) trata da importância do emprego de espões pelos governantes e generais. O mestre chinês dedica seu último capítulo inteiramente à atividade de inteligência como fator essencial para a vitória e lembra que “se um soberano iluminado e seu comandante obtêm a vitória sempre que entram em ação e alcançam feitos extraordinários, é porque eles detêm o conhecimento prévio e podem antever o desenrolar de uma guerra. (...) Este conhecimento prévio, no entanto, não pode ser obtido por meio de fantasmas e de espíritos, nem pode ser obtido com base em experiências análogas, muito menos ser deduzido com base em cálculos das posições do sol e da lua. Deve ser obtido das pessoas que, claramente, conhecem as situações do inimigo. (...) Há cinco tipos de espões que podem ser utilizados: espião nativo, espião interno, espião convertido, espião descartável e espião indispensável. (...) Quando se emprega os cinco tipos de espões simultaneamente, o inimigo não consegue desvendar os métodos de operação. É extremamente complicada e se torna uma arma mágica para o soberano derrotar seu inimigo”, Sun Tzu, *A Arte da Guerra* (Rio de Janeiro: Bibliex, 2003).

139 Para uma perspectiva mais aprofundada do controle da atividade de inteligência, inclusive com o desenvolvimento dos temas que serão apresentados a seguir vide, de nossa autoria, *Políticos e Espões – o controle da atividade de inteligência* (Niterói: Impetus, 2010).

140 Hely Lopes Meirelles, *Direito Administrativo Brasileiro*, 21ª edição (São Paulo: Malheiros, 1996), p. 574.

141 *Ibid.*, p. 574.

142 Celso Antônio Bandeira de Mello, *Curso de Direito Administrativo*, 13ª edição (São Paulo: Malheiros, 2001), p. 212.

143 Meirelles, *op. cit.*, p. 576.

144 Jans Born, “Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices”, em *Connections – Quarterly Journal*, III (dezembro 2004): pp. 1-12.

## Russell G. Swenson y Carolina Sancho Hirane

145 Greg Hannah, Kevin O'Brien, Andrew Rathmell, *Technical Report: Intelligence and Security Legislation for Security Sector Reform*, prepared for the United Kingdom's Security Sector Advisory Team, (Cambridge, RAND Europe, June 2005), p. 12.

146 Curiosamente, outro termo que não encontra tradução em português é *enforcement*.

147 Sobre os princípios que regem a Administração Pública Brasileira, vide Bandeira de Mello, *op. cit.*, Capítulo II; Meirelles, *op. cit.*, pp. 82-87; e Fernanda Marinela, *Direito Administrativo*, 4ª Edição (Niterói: Impetus, 2010), pp. 26-63.

148 Geneva Centre for the Democratic Control of Armed Forces (DCAF), DCAF Intelligence Working Group, *Intelligence Practice and Democratic Oversight – A Practitioner's View*, DCAF Occasional Paper No. 3 (Geneva, July 2003), p. 1.

149 Do encarregado de caso de determinada operação ao diretor-geral, passando pelos chefes do setor ou departamento, todos têm a obrigação de exercer o controle gerencial sobre seus subordinados.

150 Glenn P. Hastedt, ed., *Controlling Intelligence* (London: Frank Cass, 1991), p. 13.

151 DCAF Intelligence Working Group, *op. cit.*, p. 2.

152 Bruneau, *op. cit.*, pp. 23-24.

153 Thomas Bruneau e Steven Boraz, eds., *Reforming Intelligence – Obstacles to Democratic Control and Effectiveness* (Austin: University of Texas Press, 2007), p. 13.

154 Hastedt, *op. cit.*, pp. 14-15.

155 Ugarte, *op. cit.*, p. 102.

156 Marina Caparini, "Challenges of Control and Oversight of Intelligence Services in a Liberal Democracy", Geneva Centre for the Democratic Control of Armed Forces, Conference paper presented at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, Geneva, 2002.

157 Bruneau e Boraz, *op. cit.*, pp. 12-13.

158 Caparini, *op. cit.*

159 Mary Sturtevant, "Congressional Oversight of Intelligence: One Perspective", *American Intelligence Journal*, National Military Intelligence Association (Summer

## Gestão de Inteligência em las Américas

1992). Disponível em: <http://www.fas.org/irp/eprint/sturtevant.html>. Sturtevant era membro do *U.S. Senate Select Committee on Intelligence*.

160 Amy B. Zegart, “The Domestic Politics of Irrational Intelligence Oversight”, *Political Science Quarterly*, 126, no.1 (2011).

161 Caparini usa o termo “*advocate*”.

162 Reg Whitaker, “*Designing a Balance between Freedom and Security*”, em *Joseph Fletcher, ed., Ideas in Action: Essays on Politics and Law in Honour of Peter Russell* (Toronto: University of Toronto Press, 1999), pp. 144-145.

163 Caparini, *op. cit.*

164 Zegart, *op. cit.*

165 Peter Gill, “Security and Intelligence Services in the United Kingdom”, em Jean-Paul Brodeur e Dennis Tollberg, eds., *Democracy, Law and Security – Internal Security Services in Contemporary Europe* (Aldershot, UK: Ashgate Publishing Limited, 2003), p. 4.

166 José Manuel Ugarte, *Control público de la actividad de inteligencia: Europa y América Latina, una visión comparativa*, trabalho apresentado ao seminário internacional “Post-Globalización: Redefinición de la Seguridad y la Defensa Regional en el Cono Sur”, organizado pelo Centro de Estudios Internacionales para el Desarrollo, em Buenos Aires, 2002.

167 Peter Gill, *Policing Politics: Security Intelligence and the Liberal Democratic State* (London: Frank Cass, 1994), p. 251.

168 Nos modelos jurídicos de influência romano-germânica, a existência de um arcabouço legal efetivo é essencial para orientar as ações dos agentes públicos, uma vez que, em se tratando de administração pública, “o que não estiver previsto na lei, não existe”. Isso é interessante ao limitar de forma significativa a discricionariedade do agente ou administrador público. Ademais, é importante que todas as condutas determinadas aos agentes públicos estejam previstas em lei. No Brasil, por exemplo, país cujo sistema jurídico-normativo, além da origem romano-germânica, é altamente influenciado pelo positivismo do século XIX, entende-se que, enquanto no campo privado se pode fazer tudo que a lei não proíba, na esfera pública só se pode fazer aquilo que for expressamente autorizado por lei. Aspectos interessantes do modelo brasileiro relacionam-se a momentos históricos em que regimes de exceção se “legitimavam” por meio do estabelecimento de novos arcabouços legais. Nesse sentido,

pode acontecer em sistemas de influência romano-germânica que dentro do próprio Estado se produzam leis e autorizações abusivas que orientem agentes públicos.

169 Peter Gill, “A Inteligência, Controle Público e Democracia”, tradução de Maria Isabel Taveira, em Brasil, Congresso Nacional, *Anais do Seminário Atividades de Inteligência no Brasil: Contribuições para a Soberania e a Democracia, de 6 a 7 de novembro de 2002* (Brasília: Abin, 2003), p. 70.

170 *Ibid.*, p. 79.

171 Entre as fontes para a síntese que será aqui apresentada estão os trabalhos produzidos pelo *Geneva Centre for the Democratic Control of Armed Forces* (DCAF), pelo Conselho da Europa, recentes obras publicadas com estudos de casos de controle da atividade de inteligência pelo mundo e, naturalmente, a experiência prática deste autor. Informações mais detalhadas sobre orientações e práticas estão disponíveis em nosso livro *Políticos e Espiões – o controle da atividade de inteligência, op. cit.*

172 Thomas Bruneau e Kenneth Dombroski, “Reforming Intelligence: The Challenge of Control in New Democracies” (*separata*), pp. 16-17.

173 Muitos países, entre os quais EUA, Israel, França, Grã-Bretanha, Alemanha, Portugal, Rússia, adotam essa divisão entre serviços de inteligência externa e de segurança interna.

174 A título de exemplo, sugere-se consulta ao sítio do BfV, o serviço de inteligência doméstica alemão, no qual se encontra claramente a disposição das ameaças com as quais o serviço deve lidar: <http://www.verfassungsschutz.de>. Acesso 10 novembro 2011.

175 A dificuldade de fazê-lo se encontra, por exemplo, no sistema estadunidense, no caso da distribuição de competências entre a CIA e o FBI e as limitações à atuação da NSA. Apesar das melhorias na implementação de certas ações, na contra-inteligência ainda não foram resolvidos os conflitos de jurisdição, como assinala Mark Riebling em *Wedge: The Secret War between the FBI and CIA* (New York: Alfred A. Knopf, 1994).

176 Pode-se, por exemplo, estabelecer normas sobre a permanência do Diretor no cargo, como um mandato específico, ou regras para destituí-lo em caso de abuso de autoridade ou de outras condutas consideradas comprometedoras de sua função.

177 Para o inteiro teor da LAI, e do Decreto que a regulamenta, vide [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/l12527.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm) (em português).

## Gestão de Inteligência em las Américas

178 Sobre o assunto, vide os comentários do Senador e ex-Presidente da República Fernando Collor de Mello referentes ao Projeto de Lei da Câmara (PLC) Nº 41, de 2010, que deu origem à LAI ([http://www.senado.gov.br/atividade/material/detalhes.asp?p\\_cod\\_mate=96674](http://www.senado.gov.br/atividade/material/detalhes.asp?p_cod_mate=96674)) e à própria LAI, por ocasião da entrada em vigor da Lei (<http://joanisval.com/2012/05/26/ainda-sobre-a-lei-de-acesso-a-informacao/>). Também em nosso site pessoal fazemos alguns comentários sobre a LAI e suas tecnicidades ([www.joanisval.com](http://www.joanisval.com)).

179 Para a *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental mexicana* vide [www.diputados.gob.mx/LeyesBiblio/doc/244.doc](http://www.diputados.gob.mx/LeyesBiblio/doc/244.doc).

180 Sobre o assunto, vide *Mexico's Access to Information Index*, 29 abril 2010 (disponível em <http://www.article19.org/data/files/pdfs/press/mexico-access-to-information-index.pdf>. Acesso 20 maio 2012) e “O Sistema Mexicano de Transparência e Acesso à Informação Pública Governamental”, de Ernesto Isunza-Vera (texto elaborado para o Seminário regional “Sociedade civil e as novas institucionalidades democráticas na América Latina: dilemas e perspectivas”, Brasília, 9-12 de novembro de 2008, e disponível em <http://www.inesc.org.br/equipe/ivonem/MEXICO%20Acesso%20a%20informacao.pdf>. Acesso 24 maio 2012).

181 De acordo com o art. 49, I, da Constituição Brasileira, é competência exclusiva do Congresso Nacional “resolver definitivamente sobre tratados, acordos ou atos internacionais que acarretem encargos ou compromissos gravosos ao patrimônio nacional”. Com isso, qualquer tratado assinado pelo Brasil deve ser submetido à apreciação da Câmara dos Deputados e do Senado Federal antes de ser ratificado.

182 A decisão da CRE que criou o precedente se deu a partir da aprovação do relatório do Senador Aloysio Nunes Ferreira sobre o Projeto de Decreto Legislativo Nº 238, de 2011 (Nº 46, de 2011, na origem), que “aprova o texto do Acordo entre a República Federativa do Brasil e o Reino da Espanha Relativo à Segurança de Informações Sigilosas, assinado em Madri, em 17 de setembro de 2007”. O texto do relatório está disponível em <http://www6.senado.gov.br/mate-pdf/103774.pdf>. Acesso 1 maio 2012.

183 Para acessar a Lei Nº 9883, de 1999, vide [http://www.planalto.gov.br/ccivil\\_03/LEIS/L9883.htm](http://www.planalto.gov.br/ccivil_03/LEIS/L9883.htm) (em português).

184 A “ganguê dos oito” é composta pelo presidentes e vice-presidentes das comissões de inteligência da Câmara e do Senado e pelos líderes da maioria e da minoria das duas Casas.

185 National Security Act 1947, as amended, Sec. 503 [50 U.S.C. 413b] (b) and (c).



186 Sobre o assunto, vide “Sensitive Covert Action Notifications: Oversight Options for Congress”, *Congressional Research Service Report for Congress*, R40691, April 6, 2011, disponível em [http://assets.opencrs.com/rpts/R40691\\_20110406.pdf](http://assets.opencrs.com/rpts/R40691_20110406.pdf). Acesso 1 janeiro 2012; e “Gang of Four’ Congressional Intelligence Notifications” (*Congressional Research Service Report for Congress*, R40698, 18 marzo 2011, disponível em [http://assets.opencrs.com/rpts/R40698\\_20110318.pdf](http://assets.opencrs.com/rpts/R40698_20110318.pdf). Acesso 1 janeiro 2012. Ambos de Alfred Cumming.

187 Exemplo são movimentos sociais ou grupos políticos que preguem a subversão, a tomada do poder pela força ou a instabilidade institucional como meio de alcançar seus objetivos políticos.

188 Vide “Congressional Oversight of Intelligence: Current Structures and Alternatives”, de L. Elaine Halchin e Frederick M. Kaiser, *Congressional Research Service Report for Congress*, RL32525, 14 marzo 2012. Disponível em [http://assets.opencrs.com/rpts/RL32525\\_20120314.pdf](http://assets.opencrs.com/rpts/RL32525_20120314.pdf). Acesso 1 junio 2012.

189 A Constituição Brasileira de 1988 dispõe, em seu art. 50, que a “Câmara dos Deputados e o Senado Federal, ou qualquer de suas Comissões, poderão convocar Ministro de Estado ou quaisquer titulares de órgãos diretamente subordinados à Presidência da República para prestarem, pessoalmente, informações sobre assunto previamente determinado, importando crime de responsabilidade a ausência sem justificação adequada” e que os “Ministros de Estado poderão comparecer ao Senado Federal, à Câmara dos Deputados, ou a qualquer de suas Comissões, por sua iniciativa e mediante entendimentos com a Mesa respectiva, para expor assunto de relevância de seu Ministério”.

190 “A convocação de ministros é utilizada com parcimônia pelo Plenário das Casas legislativas (...). Entre 1988 e 2004, foram 201 convocações apresentadas na Câmara e 126 no Senado: um total de 344 em dezesseis anos – menos de 1 convocação por parlamentar na Câmara, e 1.5 no Senado, apesar da aparência de que a Câmara domina o cenário. (...) Relembro que as convocações de ministros e outras autoridades nas comissões, onde essa é uma prática comum, não estão incluídas.” Leany Barreiro Lemos, *Controle Legislativo em Democracias Presidencialistas: Brasil e EUA em perspectiva comparada*, Tese de Doutorado (Brasília: Universidade de Brasília, 2005), p. 89.

191 “[...] [O requerimento de informações] é feito por escrito e apresentado no plenário de uma das casas, onde é lido e submetido à votação, e deve ser aprovado por maioria simples. Os requerimentos de informação não podem conter pedido de providência, consulta, sugestão, conselho ou interrogação sobre propósito da

autoridade a quem se dirija e, para todos os efeitos, se equiparam ao pedido de remessa de documentos. A recusa ou não-atendimento do pedido no prazo de 30 dias, bem como a prestação de informações falsas, importa em crime de responsabilidade. (...) Os requerimentos de informação aparecem quantitativamente como os instrumentos “preferidos”: desde a promulgação da Constituição, em outubro de 1988, até 31 de dezembro de 2004, foram apresentados 15.341 requerimentos de informação na Câmara dos Deputados e 3.097 requerimentos de informação no Senado Federal, totalizando 18.438.” Lemos, *op. cit.*, p. 87.

192 “(...) Previstas no art. 58 da Constituição Federal de 1988, as audiências são realizadas tanto para instruir matéria, tratar de assunto de interesse público relevante, quanto para realizar o controle e poderá ser realizada inclusive por solicitação de entidade da sociedade civil, sindicatos, associações e solicitar depoimento de qualquer autoridade ou cidadão. (...) Os dados aqui apresentados cobrem todas as audiências realizadas no período de 1988 a 2004 para o Senado, e de 1995 até 2004 para a Câmara dos Deputados. No total, foram 1.495 audiências, 865 das quais ocorridas na Câmara e 630 no Senado, exclusivamente no seu sistema de comissões.” Lemos, *op. cit.*, pp. 91-92.

193 “Um incentivo para o uso dos requerimentos é o baixo custo para sua apresentação. É uma ação predominantemente individual. Basta apresentar sua proposição, que será lida e aceita, e posteriormente encaminhada ao ministério ou órgão devidos. (...) Não há, portanto, a necessidade de negociar nas instâncias formais –lideranças, comissões, blocos, partidos– o apoio para essa iniciativa, ou que submeter a voto de maioria. O requerimento também não altera *o status quo* e, assim, o Congresso não incorre também no risco de alterar as políticas públicas numa direção desconhecida. Não gera obrigações ou custos. Isso não quer dizer que não seja uma ação real de controle. Ele pode ser um instrumento estratégico de importância, ao abordar assuntos sensíveis, e para se barganhar ações legislativas ou alocação de recursos.” Lemos (2005), *op. cit.*, pp. 87-88.

194 Ressalte-se que a prática no Congresso não é de convocar ministros de Estado – medida vista como de significativo desgaste, pois seu descumprimento enseja crime de responsabilidade. Para evitar o constrangimento desnecessário de autoridades do executivo, costuma-se substituir a convocação pelo “convite” para audiências públicas ou sessões reservadas. As autoridades do executivo, ao menos as da áreas de inteligência, costumam atender prontamente aos convites do poder legislativo. Sobre o assunto, vide Lemos, *op. cit.*, e Maria Helena de Castro Santos, “Controles parlamentares e os militares no Brasil: audiências públicas e requerimentos de informações, 1995-2004”, em Mariana Llanos, Ana Maria Mustapic, (orgs.), *Controle*

*Parlamentar na Alemanha, na Argentina e no Brasil* (Rio de Janeiro: Fundação Konrad Adenauer, 2005), pp. 113-139.

195 Isso já aconteceu, por exemplo, no Canadá, quando uma comissão de parlamentares (e não uma comissão parlamentar ou “do Parlamento”) foi criada para fiscalizar questões relacionadas à comunidade de segurança e inteligência. A comissão acabou muito limitada em suas ações e atuou conforme os interesses e orientações do Governo, ou seja, do Primeiro-Ministro. A esse respeito, vide Stuart Farson, “Parliament and its Servants: Their Role in Scrutinizing Canadian Intelligence”, em David Stafford e Rhodri Jeffreys-Jones, (eds.), *American-British-Canadian Intelligence Relations 1939-2000* (London: Frank Cass, 2000), p. 243 e ss.

196 Tratam-se de medidas de garantia da independência da comissão de controle.

197 Sobre o assunto, vide Zegart, *op. cit.*

198 “6. (1) *The Director, under the direction of the Minister, has the control and management of the Service and all matters connected therewith.* (2) *In providing the direction referred to in subsection (1), the Minister may issue to the Director written directions with respect to the Service and a copy of any such direction shall, forthwith after it is issued, be given to the Review Committee.*” CSIS Act, section 6, (1), (2).

199 “*The CSIS Act established, in law, a comprehensive regime for the security intelligence function in Canada: a civilian agency with no executive terms of reference; with clearly (and where appropriate, precisely) defined mandate and powers; subject to a rigorous, inter-related system of political and judicial controls; and, importantly, subject to independent, arm’s-length review. The centrepiece of that system for accountability, control and review was and is the unique combination of the Security Intelligence Review Committee (SIRC) and the Inspector General (IG) — the former reporting, through the Minister, to Parliament; the latter, in a more specialized but complementary way, acting as the Minister’s ‘eyes and ears’ on the Service*”, Canadian Security Intelligence Service, Backgrounder N° 17, *Control, Accountability and Review*, May 2005. Disponível em <http://www.csis.gc.ca/en/newsroom/backgrounders/backgrounder17.asp>. Acesso 25 fevereiro 2012.

200 “*The Security Intelligence Review Committee is the only body with the legal mandate and expertise to carry out ongoing, independent review of the activities of CSIS. SIRC was established under the CSIS Act (1984) to provide assurance to the Parliament of Canada and to Canadians that CSIS is acting in accordance with the law, policy and Ministerial Direction in the performance of its duties and functions. In doing so, SIRC seeks to ensure that CSIS respects the fundamental rights and freedoms of Canadians.*”

## Gestión de Inteligencia en las Américas

Canada, Security Intelligence Review Committee (SIRC), *SIRC Annual Report 2006–2007 – An Operational Review of the Canadian Security Intelligence Service* (Ottawa: Public Works and Government Services Canada, 2007), p. 3.

201 Essas funções do CSIS estão definidas nas seções 12 a 17 do CSIS Act.

202 “SIRC recognizes that the conduct of security intelligence agencies can prompt impassioned debate about whether the ends can ever justify the means. We also have first-hand knowledge that there are individuals who will seek to exploit Canada’s rights and freedoms in order to harm our country, our citizens and our neighbors and friends around the world. (...) SIRC recognizes that police and security intelligence agencies in the post 9/11 world must deal with daunting challenges, including globalized and technologically sophisticated terrorist groups. We also know that the relative safety that Canadians enjoy is thanks in large part to the efforts of these same agencies on our behalf. But the obligation to ensure public safety ought not to reduce in any way respect for the rule of law”, *SIRC Annual Report 2006-2007*, pp. v-vi.

203 “40. For the purpose of ensuring that the activities of the Service are carried out in accordance with this Act, the regulations and directions issued by the Minister under subsection 6(2) and that the activities do not involve any unreasonable or unnecessary exercise by the Service of any of its powers, the Review Committee may (a) direct the Service or Inspector General to conduct a review of specific activities of the Service and provide the Committee with a report of the review; or (b) where it considers that a review by the Service or the Inspector General would be inappropriate, conduct such a review itself”, *CSIS Act, section 40*.

204 *CSIS Act*, seções 41 a 46.

205 Artículo 15 de la Ley de Defensa Nacional de 1988 destaca conceptos de defensa nacional y seguridad interna, y prohíbe la participación de la inteligencia de las Fuerzas Armadas en asuntos relacionados con temas de política interna.

206 “Predator Drones and Unmanned Aerial Vehicles”, *New York Times*, 30 julio 2012 (actualizado). Disponible en [http://topics.nytimes.com/top/reference/timestopics/subjects/u/unmanned\\_aerial\\_vehicles/index.html](http://topics.nytimes.com/top/reference/timestopics/subjects/u/unmanned_aerial_vehicles/index.html). Consultado 15 agosto 2012. Véase también, “How the Pentagon’s Top Killers Became (Unaccountable) Spies”, *Wired Magazine*, 13 febrero 2012. Disponible en [www.wired.com/dangerroom/2012/02/joc-ambinder/](http://www.wired.com/dangerroom/2012/02/joc-ambinder/). Consultado 15 agosto 2012.

207 Según U.S. Congress, Fiscal Year 2010 Intelligence Authorization Act, Ley Pública 111–259, 7 octubre 2010, Section 326, Subtitle D. Disponible en <http://intelligence.senate.gov/pdfs/111th/111259.pdf>. Consultado 15 agosto 2012.

208 El acto de 1978 controla solamente acciones de seguimiento, por parte de organismos de la comunidad de inteligencia de los EEUU, dentro del país. Para esbozo del Acto de 1978 y sus enmiendas, véase sitio del Center for National Security Studies en <http://www.cnss.org/ffisa.htm>. Consultado 15 agosto 2012.

209 Gregory Weeks, "A Preference for Deference: Reforming the Military's Intelligence Role in Argentina, Chile and Peru", *Third World Quarterly* 29, no. 1 (2008), p. 57.

210 "El término 'ética' deriva de la palabra griega que significa 'costumbre' y, por ello, se ha definido con frecuencia la ética como la doctrina de las costumbres, sobre todo en las direcciones empiristas. Las virtudes éticas son para Aristóteles aquellas que se desenvuelven en la práctica y que van encaminadas a la consecución de un fin, en tanto que las dianoéticas son las virtudes propiamente intelectuales. En la evolución posterior del sentido del vocablo, lo ético se ha identificado cada vez más con lo moral, y la ética ha llegado a significar propiamente la ciencia que se ocupa de los objetos morales en todas sus formas, la filosofía moral". Mientras que "moral se deriva de *mos*, costumbre, lo mismo que 'ética' de ἦθος y por eso 'ética' y 'moral' son empleados a veces indistintamente. En algunas lenguas, y en español entre ellas, lo moral se opone a lo físico, y de ahí que las ciencias morales comprendan, en oposición a las ciencias naturales, todo lo que no es puramente físico en el hombre (la historia, la política, el arte, etc.), es decir, todo lo que corresponde a las producciones del espíritu subjetivo y aun el espíritu subjetivo mismo. Y, finalmente, lo moral se opone comúnmente a lo inmoral y a lo amoral en cuanto lo que se halla insertado en el orbe ético se opone a lo que se enfrenta con este orbe o permanece indiferente ante él. Lo moral es en tal caso lo que se somete a un valor, en tanto que lo inmoral y lo amoral son, respectivamente, lo que se opone a todo valor y lo que es indiferente al valor". En José Ferrater Mora, *Diccionario de la Filosofía*, 5<sup>a</sup> edición (Buenos Aires: Editorial Sudamericana, 1964), vol. I, pp. 594-595, y vol. II, pp. 232-233.

211 La lista de autores es larga. Muchos fueron o siguen siendo miembros de la comunidad de inteligencia estadounidense; otros enseñan e investigan en universidades de América del Norte y Europa Occidental, o son altos funcionarios de gobierno de reputadas democracias occidentales. Algunos de ellos se encuentran citados en este trabajo: Stefan Brem, Jan Goldman, Melvin Goodman, Albert Pierce, Erich Schmidt-Eenboom y Brian Snow.

212 Hasta ahora lamentablemente, tanto en sus conferencias como en su revista, la IIEA nunca ha tratado temas sobre América Latina. En este artículo se han revisado varios trabajos publicados por ella.

## Gestión de Inteligencia en las Américas

213 Allison M. Shelton, "Framing the Oxymoron: A New Paradigm for Intelligence Ethics", *Intelligence and National Security* 26, no. 1 (2011), p. 25.

214 Jan Goldman, "Ethics Phobia and the US Intelligence Community: Just Say 'No', A Symposium on Intelligence Ethics", *Intelligence and National Security* 24, no. 3 (2009), p. 374. Este autor, profesor en el National Defense Intelligence College en Washington D.C., considera que "eticafobia" es el miedo a la contemplación del tema de una conducta ética.

215 Shelton, *op. cit.*, pp. 28-30.

216 *Ibid*, p. 26.

217 Tony Pfaff y Jeffrey R. Tiel, "The Ethics of Espionage", *Journal of Military Ethics* 3, no. 1 (2004), pp. 11-14.

218 *Ibid*, pp. 14-15.

219 Melvin A. Goodman, *Revamping the CIA, Issues in Science and Technology Online* (invierno 2001). Disponible en <http://www.issues.org/18.2/goodman.html>. Consultado 23 Agosto 2012.

220 U.S. Senate, *Alleged Assassination Plots Involving Foreign Leaders: An Interim Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities* (Washington, DC: U.S. Government Printing Office, 20 noviembre 1975), pp. 257-258. Disponible en [http://www.aarclibrary.org/publib/church/reports/ir/pdf/ChurchIR\\_4\\_Findings.pdf](http://www.aarclibrary.org/publib/church/reports/ir/pdf/ChurchIR_4_Findings.pdf). Consultado 23 agosto 2012.

221 Elizabeth B. Bazan, "Assassination Ban and E.O. 12333: A Brief Summary", *Congressional Research Service Report* RS21037, 4 enero 2002, pp. 1-3.

222 Melvin A. Goodman, "CIA Failures of Tradecraft and Intelligence Prior to the Second Iraq War", en *Intelligence Ethics: The Definitive Work of 2007*, Michel Andregg, ed. (St. Paul, Minnesota: Center for the Study of Intelligence and Wisdom, 2007), p. 32. Disponible en <http://www.gzmn.org/pdfonline/IntelligenceEthics2007-MA.pdf>. Consultado 23 agosto 2012.

223 Erich Schmidt-Eenboom, "Geheimdienste in Demokratien", *Weltrends: Zeitschrift für internationale Politik und vergleichende Studien* 14, no. 51 (2006), p. 17.

224 *Ibid*, pp. 14-23.

225 Schlächter von Lyon, “Nazi-Verbrecher Barbie war BND-Agent”, *Der Spiegel*, 15 enero 2011; y Michael Kimmelman, “50 Years After Trial, Eichmann Secrets Live On”, *New York Times*, 5 septiembre 2011.

226 Stefan Brem, “Special Ethics for Special Services”, en *Intelligence Ethics: The Definitive Work of 2007*, Michael Andregg, ed., *op. cit.*, pp. 11-13. Las 10 directrices pueden encontrarse en [http://www.echr.coe.int/NR/rdonlyres/176C046F-C0E6-423C-A039-F66D90CC6031/0/LignesDirectrices\\_EN.pdf](http://www.echr.coe.int/NR/rdonlyres/176C046F-C0E6-423C-A039-F66D90CC6031/0/LignesDirectrices_EN.pdf). Consultado 23 agosto 2012.

227 Schmidt-Eenboom, *op. cit.*, p. 24.

228 Brian Snow, “Intelligence Community ‘Mission Ethics’: A Symposium on Intelligence Ethics”, *Intelligence and National Security* 24, no. 3 (2009), p. 385.

229 “El CNI prepara un ‘código ético’ del agente secreto”, *ABC*, Madrid, 25 junio 2010.

230 “El código ético de los espías estará listo en primavera”, *El Confidencial Digital*, Madrid, 7 marzo 2011.

231 “El código ético del CNI”, *El Confidencial Digital*, Madrid, 12 enero 2012.

232 Albert C. Pierce, “The Value of an Ethos for Intelligence Professionals”, en *Intelligence Ethics: The Definitive Work of 2007*, Michael Andregg, ed., *op. cit.*, pp. 9-10.

233 Florina Cristiana Matei y Thomas Bruneau, “Explaining Failures and Successes in the Democratization of Intelligence”, Panel sobre “Politics of Intelligence Governance” en The ECPR’S General Conference, Potsdam, Alemania, 10-12 Septiembre 2009, pp. 2-3.

234 Rafael José de Espona, “Los servicios de inteligencia en los países post-soviéticos”, *Inteligencia y Seguridad* 8 (2010), p. 77.

235 Julia Pulido Gragera, *Los servicios de inteligencia rusos: Influencia de la nueva Rusia en el actual sistema de seguridad* (Madrid: Centro Superior de Estudios de la Defensa Nacional, 2010), pp. 138-143.

236 Matei y Bruneau, *op. cit.*, pp. 15 y sigs.

237 Carlos Maldonado Prieto, “Desafíos de los servicios de inteligencia en la región andina”, en *SIN Arcana imperii: Inteligencia en democracia*, Andrés Gómez de la Torre Rotta, ed. (Lima: Foro Libertad & Seguridad, 2007), p. 267.

## Gestión de Inteligencia en las Américas

238 Carlos Maldonado Prieto, “Dilemas antiguos y modernos en la inteligencia estratégica en Sudamérica”, *Security and Defense Studies Review* 9 (2009), p. 54.

239 “Creación de nueva Agencia Nacional de Inteligencia recibe apoyo del Gobierno Británico”, Radio Santa Fe, Bogotá, 9 noviembre 2011. Efectivamente, el Presidente Juan Manuel Santos y el asesor para la seguridad nacional, Sergio Jaramillo, se reunieron en Londres a fines de noviembre de 2011 con John Sawyer, director del MI6. Véase <http://unidad-intel-latinoamerica.webnode.com.ar/news/presidente-santos-crea-nueva-agencia-de-inteligencia-colombiana-con-apoyo-del-reino-unido-/>. Consultado 23 agosto 2012.

240 “Colombia crea una nueva agencia de inteligencia tras haber liquidado anterior”, *EFE*, 4 noviembre 2011.

241 También se señala que en ningún caso la información de inteligencia y contrainteligencia será recolectada, procesada o diseminada por razones de género, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica, pertenencia a una organización sindical, social o de derechos humanos, o para promover los intereses de cualquier partido o movimiento político o afectar los derechos y garantías de los partidos políticos de oposición. En Ley de Inteligencia y Contrainteligencia de Colombia. Véase <http://colarebo.files.wordpress.com/2011/05/ley-de-inteligencia-y-contrainteligencia-pdf.pdf>. Consultado 23 agosto 2012.

242 La obediencia debida se entendió tradicionalmente en América Latina como una situación que exime de responsabilidad penal por delitos cometidos en el cumplimiento de una orden impartida por un superior jerárquico en el ámbito castrense, a la que el subordinado no puede sustraerse. Sin embargo, luego de las dictaduras militares de las décadas de 1970 y 1980, la jurisprudencia cambió radicalmente, adaptándose al derecho internacional humanitario que no reconoce a la obediencia debida como eximente de responsabilidad penal.

243 Ley de Inteligencia y Contrainteligencia de Colombia. Disponible en <http://www.colarebo.files.wordpress.com/2011/05/ley-de-inteligencia-y-contrainteligencia-pdf.pdf>. Consultado 23 agosto 2012.

244 Fredy Rivera, “La Inteligencia ecuatoriana: Tradiciones, cambios y perspectivas”, en su *Inteligencia Estratégica y Prospectiva*, op. cit., pp. 62-63.

245 *Ibid*, pp. 59-60.

246 Carlos Maldonado Prieto, “La sublevación policial en Ecuador”, *Revista Atenea Digital*, 2 octubre 2010. Disponible en <http://www.ateneadigital.es/RevistaAteneal>



REVISTA/articulos/GestionNoticias\_3055\_ESP.asp; y Carlos Maldonado Prieto, “Desafíos para la Inteligencia Estratégica Latinoamericana”, *Revista Atenea Digital*, 26 noviembre 2010. Disponible en <http://www.ateneadigital.es/RevistaAteneal> REVISTA/articulos/GestionNoticias\_3432\_ESP.asp. Consultados 23 agosto 2012.

247 Corte Interamericana de Derechos Humanos, Demanda en el caso de Humberto Antonio Palamara Iribarne (Caso 11.571) contra la República de Chile, 13 de abril de 2004.

248 Humberto Palamara, *Ética y servicios de inteligencia* (Valparaíso, Armada de Chile, 2006), pp. 65-66.

249 Giorgio Del Vecchio, *Crisis del derecho y crisis del Estado* (Madrid, Librería General de Victoriano Suarez, 1935), p. 96.

250 José Luis Cea Egaña, “Estado constitucional de derecho, nuevo paradigma jurídico”, *Anuario de Derecho Constitucional Latinoamericano*, N° 11 (2005), pp. 47-50.

251 Norberto Bobbio, *Estado, gobierno y sociedad. Por una teoría general de la política* (México DF: Fondo de Cultura Económica, 2006).

252 Véase Lucía Meza y Daniel Soto, “Seguridad, derechos humanos y democracia: ¿un nuevo paradigma?”, *Revista IIDH, Instituto Interamericano de Derechos Humanos*, N°49 (2010), pp. 239-263.

253 Diego Torrente, *Desviación y delito* (Madrid, Alianza Editorial, 2001).

254 Fernando Velasco Fernández, “Democracia y Servicios de Inteligencia: Ética para qué?”, in José Luís González Cussac (coord.), *Inteligencia* (Valencia, Tirant Lo Blanch, 2012), p. 464.

255 *Ibid*, p. 474.

256 Véase Mark Riebling, *Wedge: The Secret War between the FBI and CIA* (New York: Alfred A. Knopf, 1994), pp. 121-125.

257 José González Cussac, Beatriz Larriba Hinojar y Antonio Fernández Hernández, “Servicios de Inteligencia y Estado de Derecho”, en José Luís González Cussac (coord.), *op. cit.*, pp. 283-287.

258 LA VIDA DE LOS OTROS, [DVD]. Florian Henckel von Donnersmarck, Alemania, Wiedermann & Berg Filmproduktion, Bayerischer Rundfunk, Arte y Creado Film: 2006.

## Gestión de Inteligencia en las Américas

259 EL SECRETO DE SUS OJOS, [DVD]. Juan José Campanella, Argentina, Tornasol Films, Haddock Film, 100 Bares, Telefe y otros: 2009.

260 QUÉMESE DESPUÉS DE LEERSE, [DVD]. Joel y Ethan Coen. Estados Unidos, Bronx Community College, University Avenue at West 181 Street, Bronx, New York City y otros: 2008.

261 EL DIA DEL JUICIO FINAL, [DVD]. Gregor Jordan, Estados Unidos, Lleju Productions and Films y Sidney Kimmel Entertainment International: 2009.

262 González, Larriba y Fernández, *op. cit.*, p. 316.

263 Naciones Unidas, *Derechos humanos y aplicación de la ley, Manual de capacitación en derechos humanos para policía* (Ginebra, Alto Comisionado para los Derechos Humanos, Centro de Derechos Humanos, 1997), pp. 59-66.

264 Pacto Internacional de Derechos Civiles y Políticos (artículo 13.3) y Convención Americana (artículo 22.3).

265 Declaración Universal de Derechos Humanos (artículo 20), Pacto Internacional de Derechos Civiles y Políticos (artículo 20), Declaración Americana de los Derechos y Deberes del Hombre (artículo XXII), Convención Americana sobre Derechos Humanos (artículo 16), Pacto Internacional de Derechos Económicos, Sociales y Culturales (artículo 8), Convenio 87 sobre la libertad sindical y la protección del derecho de sindicación (artículos 2 a 5), Convención sobre los Derechos del Niño (artículo 15), Convención internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares (artículos 26 y 40).

266 Declaración Universal de Derechos Humanos (artículos 10 y 11), Declaración Americana de Derechos y Deberes del Hombre (artículo XVIII y XXVI), Pacto Internacional de Derechos Civiles y Políticos (artículo 14 y 15), Convención Americana sobre Derechos Humanos (artículos 8 y 9), Convención sobre los Derechos del Niño (artículo 40) y Conjunto de Principios para la protección de todas las personas sometidas a cualquier forma de detención o prisión (principio 17).

267 CONTACTO EN FRANCIA, [DVD]. William Friedkin. Estados Unidos, D'Antoni Productions, Schine-Moore Productions: 1971.

268 Declaración Universal de Derechos Humanos (artículos 6 y 12), Pacto Internacional de Derechos Civiles y Políticos (artículos 16, 17), Declaración Americana de los Derechos y Deberes del Hombre (artículos V, IX, X, XVII), Convención

## Russell G. Swenson y Carolina Sancho Hirane

Americana sobre Derechos Humanos (artículos 3, 11 y 14), Convención sobre los Derechos del Niño (artículo 16).

269 Adoptado por la Asamblea General de Naciones Unidas en su Resolución 34/169 de 17 diciembre 1979.

270 Declaración Universal de Derechos Humanos (artículo 10 y 11), Declaración Americana de Derechos y Deberes del Hombre (artículos XVIII y XXVI), Pacto Internacional de Derechos Civiles y Políticos, artículos 14 y 15), Convención Americana sobre Derechos Humanos (artículos 8 y 9).

271 Naciones Unidas, op. cit., p. 63.

272 LOS INFILTRADOS, [DVD]. Martin Scorsese. Estados Unidos, Warner Bros. Pictures, Plan B Entertainment, Initial Entertainment: 2006.

273 Declaración Universal de Derechos Humanos (artículo 12), Pacto Internacional de Derechos Civiles y Políticos (artículo 17), Declaración Americana de los Derechos y Deberes del Hombre (artículo IX), y Convención Americana sobre Derechos Humanos (artículo 11).

274 Declaración Universal de Derechos Humanos (artículo 11), Declaración Americana de Derechos y Deberes del Hombre (artículo XXVI), Pacto Internacional de Derechos Civiles y Políticos (artículo 14.2), Convención Americana sobre Derechos Humanos.

275 Daniel O'Donnel, *Derecho internacional de los derechos humanos. Normativa, jurisprudencia y doctrina de los sistemas universal e interamericano* (Santiago, Oficina Regional para América Latina y el Caribe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2007), p. 526.

276 María Eugenia Ullman et al., *Derechos Humanos, Seguridad Ciudadana y Funciones Policiales: Módulo instruccional* (San José, Costa Rica: Instituto Interamericano de Derechos Humanos, 2011), pp. 85-89.

277 LA CIUDAD DE LAS TORMENTAS, [DVD]. Paul Greengrass. Estados Unidos, Universal Pictures, Studio Canal y Relativity Media: 2010.

278 Declaración Universal de Derechos Humanos (artículo 5); Declaración Americana de los Derechos y Deberes del Hombre (artículos I, XXV, XXVI); Pacto Internacional de Derechos Civiles y Políticos (artículos 7 y 10); Convención Americana sobre Derechos Humanos (artículo 5); Convención contra la Tortura y otros

## Gestión de Inteligencia en las Américas

Tratos o penas Crueles, Inhumanos o Degradantes; Convención Interamericana para Prevenir y Sancionar la Tortura, Reglas mínimas para el tratamiento de los reclusos; Conjunto de principios para la protección de todas las personas sometidas a cualquier forma de detención o prisión; Principios básicos para el tratamiento de los reclusos; y Reglas de las Naciones Unidas para la protección de los menores privados de libertad.

279 Pacto Internacional de Derechos Civiles y Políticos (artículo 9.2) y Convención Americana sobre Derechos Humanos (artículo 7.4).

280 Declaración Americana de los Derechos y Deberes del Hombre (artículo XXV párrafo 2), Pacto Internacional de Derechos Civiles y Políticos (artículo 10) y Convención Americana sobre Derechos Humanos (artículo 5 párrafo 2).

281 LA BATALLA DE ARGEL, [DVD]. Gillo Pontecorvo. Italia y Argelia, Igor Fil y Casbah Film: 1966.

282 Central Intelligence Agency, “Does the CIA spy on Americans? Does it keep a file on you?” Disponible en <https://www.cia.gov/about-cia/faqs/index.html#spyonamericans>. Consultado 17 abril 2011.

283 La Convención contra la Tortura y Otros Tratos o penas Crueles, Inhumanos o Degradantes de 1984 establece en su artículo 1: “A los efectos de la presente Convención, se entenderá por el término “tortura” todo acto por el cual se inflija intencionadamente a una persona dolores o sufrimientos graves, ya sean físicos o mentales, con el fin de obtener de ella o de un tercero información o una confesión, de castigarla por un acto que haya cometido, o se sospeche que ha cometido, o de intimidar o coaccionar a esa persona o a otras, o por cualquier razón basada en cualquier tipo de discriminación, cuando dichos dolores o sufrimientos sean infligidos por un funcionario público u otra persona en el ejercicio de funciones públicas, a instigación suya, o con su consentimiento o aquiescencia. No se considerarán torturas los dolores o sufrimientos que sean consecuencia únicamente de sanciones legítimas, o que sean inherentes o incidentales a éstas”. La Convención Interamericana para Prevenir y Sancionar la Tortura de 1985 define en el artículo 2: “Para los efectos de la presente Convención se entenderá por tortura todo acto realizado intencionalmente por el cual se inflijan a una persona penas o sufrimientos físicos o mentales, con fines de investigación criminal, como medio intimidatorio, como castigo personal, como medida preventiva, como pena o con cualquier otro fin. Se entenderá también como tortura la aplicación sobre una persona de métodos tendientes a anular la personalidad de la víctima o a disminuir su capacidad física o mental, aunque no causen dolor físico o angustia psíquica” ... “No estarán

comprendidos en el concepto de tortura las penas o sufrimientos físicos o mentales que sean únicamente consecuencia de medidas legales o inherentes a éstas, siempre que no incluyan la realización de los actos o la aplicación de los métodos a que se refiere el presente artículo”.

284 Pablo Bonorino afirma que el liberalismo aborrece la tortura por su íntima conexión con la tiranía y porque constituye la negación más extrema de la dignidad humana. Mediante ella el torturador aplasta, aterroriza y humilla a su víctima con el propósito de dominarla mediante el dolor. Este ha sido el objetivo de su uso tras las victorias militares, como mecanismo de dominación política mediante el terror, como castigo y como procedimiento de extracción de confesiones en la justicia absolutista. Véase Pablo Bonorino Ramirez, “Retorno de la tortura: la carga ideológica de la ficción televisiva”, *Revista Académica*, N° 51 (2011), pp. 111-112.

285 *Ibid*, pp. 109-125.

286 Humberto Antonio Palamara Iribarne demandó al Estado de Chile porque en 1993, mientras se desempeñaba como empleado civil de la Armada, se le prohibió publicar su libro “Ética y Servicios de Inteligencia”. La publicación no autorizada del texto y las declaraciones públicas de disconformidad efectuadas por el autor en contra de la actuación del Juzgado Naval de Magallanes, le significaron la incautación de los ejemplares, la eliminación de la información del disco duro de su computador, prisión preventiva por 11 días y la condena definitiva por los delitos de “incumplimiento de deberes militares”, “desobediencia” y “desacato”. La Corte Interamericana de Derechos Humanos (Corte IDH) condenó al Estado de Chile a reformar la justicia militar. (*Caso Palamara Iribarne vs. Chile* (2005): Corte Interamericana de Derechos Humanos, 22 noviembre 2005).

287 Humberto Antonio Palamara Iribarne, *Ética y Servicios de Inteligencia* (Valparaíso: Armada de Chile, 2006), p. 147.

288 Amalio Blanco Abarca, “La Condición de ‘Enemigo’: El Ocaso de la Inocencia,” en Manuel Cancio Meliá and Laura Pozuelo Pérez, (coords.), *Política Criminal en Vanguardia: Inmigración Clandestina, Terrorismo, Criminalidad Organizada* (Navarra, Spain: Editorial Aranzadi SA, 2008), pp. 257-258.

289 Henri Tajfel, *Human Groups and Social Categories: Studies in Social Psychology* (Cambridge: Cambridge University Press, 1981), p. 145.

290 Blanco Abarca, *op. cit.*, pp. 292-293.

## Gestión de Inteligencia en las Américas

291 Amartya Sen, *Identity and Violence: The Illusion of Destiny* (New York, W. W.: Norton & Company, 2007), pp. 1-8.

292 Younger-Yusuf reprocha a sus captores: “*Do it! Do it! I love my country, you people crap on it! I love my religion, you people spit on it! Just remember something, I’m here because I wanna be here! I let myself be caught, because I’m not a coward! I chose to meet my oppressors face to face! You call me a barbarian? Then what are you? What, you expect me to weep over 50 civilians? You people kill that number every day! How does it feel Brody? This is not about me! This is about you! How does it feel? You have no authority here! None! There is but one authority, and it is not you! You are a blight, you are a cancer! How does it feel Brody?*”

293 Sen, *op. cit.*, p. 175.

294 Alias “H”: “*There is no H. and Younger... there’s only victory and defeat. The winner gets to take the moral high-ground, because they get to write the history books. The loser... just loses. The only miscalculation in your plan... was me*”.

295 Albert Bandura, “Moral Disengagement in the Perpetration of Inhumanities”, *Personality and Social Psychology Review*, 3, no. 3 (1999): p. 200.

296 Véase Bandura, *op. cit.*

297 Jack Saunders, el director del FBI y jefe de Helen Brody exclama en su desesperación: “*If those bombs go off there will be no f\*#@ing Constitution!*”

298 En noviembre de 2012 el Ministro de Seguridad de Argentina, Sergio Berni, ante la captura de un presunto traficante precisó que: “que una vez que los cuerpos de inteligencia de Argentina descubrieron que López Londoño había ingresado al país a fines del año pasado, comenzó la investigación para dar con su paradero”. De <http://www.animalpolitico.com/2012/11/capturan-al-narco-mas-importante-del-mundo/>. Consultado 23 enero 2014.

En Colombia fue capturado en noviembre de 2013 un ex paramilitar, al respecto la prensa señaló sobre la captura que: “Desde la Dirección de Inteligencia de la Policía (DIPOL), informaron que sus gustos por el dinero, la buena comida y las mujeres siempre representaron su punto débil”. De [http://www.r Depp.com.pe/2013-12-08-narcotraficante-colombiano-pantera-cayo-por-tener-tres-mujeres-noticia\\_653495.html](http://www.r Depp.com.pe/2013-12-08-narcotraficante-colombiano-pantera-cayo-por-tener-tres-mujeres-noticia_653495.html). Consultado 23 enero 2014.

Durante 2011 el Ministro de Gobernación de México, Alejandro Poiré dio a conocer la “Operación Huesped”, para detener al hijo de Muammar Gaddafi, Saadi.

Al respecto el ex ministro señaló que: “los servicios de inteligencia civil mexicanos detectaron un plan de internación ilegal de Saadi Gaddafi y de su familia a México, para lo cual se procedió conforme a los protocolos y los procedimientos correspondientes”. De <http://www.cronica.com.mx/notas/2012/620994.html>. Consultado 24 enero 2014.

299 Ver las diferentes versiones de los Libros Blancos de Defensa de países de América Latina. Ver en: [www.resdal.org](http://www.resdal.org).

300 La calidad de país emergente se reconoce a partir de sus características económicas y los altos estándares de desarrollo que los indicadores internacionales evidencian. Implica un proceso de reforma y transformación en el ámbito financiero, económico, social, laboral, tributario y del sector público.

301 Ver José Manuel Ugarte, “Las estructuras de inteligencia en América Latina”, *Foreign Affairs en Español* (primavera 2002), p. 60; Carlos Maldonado, “Servicios de Inteligencia en Sudamérica: Estado de situación en perspectiva comparada”, Instituto de Cooperación para la Seguridad Hemisférica -WHINSEC, (Fort Benning, Georgia, Estados Unidos: junio de 2002).

302 Ver Russell G. Swenson y Susana Lemozy, (coords.), *Profesionalismo de Inteligencia en las Américas* (Washington, DC: Joint Military Intelligence College, 2004).

303 La Gobernanza se ha transformado en un concepto operacional destinado a evaluar el comportamiento y evolución de las democracias conforme indicadores que dan cuenta de su capacidad de adaptabilidad y cumplimiento de parámetros internacionales para expresar la solidez institucional de los países. América Latina avanza en responder a las nuevas formas de evaluar el régimen democrático de distintas maneras. Ver <http://info.worldbank.org/governance/wgi/index.asp>.

304 Los mayores requerimientos se concentran en las actividades asociadas a crimen organizado, incluyendo terrorismo, narcotráfico, lavado de activos entre varios otros. Respecto de ellos, la interacción con organismos extranjeros se hacen directamente con los encargados de cada tema en las organizaciones respectivas, sean policiales, militares u otras.

305 A riesgo de ser redundante, cuando nos referimos a la relación entre inteligencia y política, lo hacemos considerando la forma en que se usa la producción de inteligencia nacional en la toma de decisiones del gobernante, considerando que la seguridad, en su amplio espectro de preocupaciones, es un pilar del desarrollo.

## Gestión de Inteligencia en las Américas

306 Entre otros: Michael Hermann, *Intelligence Power in Peace and War* (Cambridge: Cambridge University Press, 1996); Richards K. Betts, *Enemies of Intelligence* (New York: Columbia University Press, 2007). El Centro Sherman Kent para Analisis de Inteligencia tiene varios trabajos sobre el tema. Ver para el caso de América Latina: Thomas C. Bruneau and Steven C. Boraz, eds., *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness* (Austin: University of Texas Press, 2007). También Russell G. Swenson y Susana C. Lemozy, (coords.), *Democratización de la Función de Inteligencia: El Nexo de la Cultura Nacional y la Inteligencia Estratégica* (Washington, DC: National Defense Intelligence College, 2009); José Manuel Ugarte, 2002, *op. cit.*, p. 60.; Carlos Maldonado, 2002, *op. cit.*

307 Ohad Leslau, "The Effect of Intelligence on the Decisionmaking Process", *International Journal of Intelligence and Counterintelligence* 23 no. 3 (2010), pp. 426-448.

308 Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston: Little Brown, 1972).

309 Ver Yaacov Y.I. Vertzberger, "Bureaucratic-Organizational Politics and Information Processing in a Developing Country", *International Studies Quarterly*, vol. 28, no. 1 (1984), pp. 69-95.

310 Las estructuras de asesoría presidencial de EE.UU., Francia y Reino Unido suelen ser señalados como ejemplos de sistemas exitosos, donde se incorpora en términos amplios y regulados el aporte de los productos del sistema de inteligencia. En América Latina el aporte del sistema de inteligencia están escasamente regulados y hay poca bibliografía al respecto. Una aproximación general se ve en: Deborah Stone, *Policy Paradox. The Art of Political Decision Making*, edición revisada (New York y London: Norton & Company, 2002); Michael Nelson, ed., *The Presidency and the Political System*, 9th. ed. (Washington, DC: CQ Press, 2010); Michelangelo Vercesi, "Cabinets and Decision-Making Processes: Re-assessing the Literature", en *Journal of Comparative Politics* vol. 5, no. 2 (julio 2012), disponible en <http://www.cuppi.si/assets/jcp/JCP-Issue-8-July-2012.pdf>. Para el caso de Chile ver Maria de los Angeles Fernández y Eugenio Rivera Urrutia, eds., *La Trastienda del Gobierno* (Santiago de Chile: Catalonia, 2012). La conformación de estructuras funcionales de apoyo al proceso de decisión a nivel presidencial es un tema pendiente en la bibliografía asociada al rol y función de los sistemas de inteligencia en América Latina.



## Russell G. Swenson y Carolina Sancho Hirane

311 Entendemos por inteligencia estratégica la producción de conocimiento sobre áreas o problemas vitales para el interés nacional, con el fin de asesorar al más alto nivel político a fin de anticipar, prevenir y resolver situaciones de amenaza o riesgo para el estado democrático.

312 Russell G. Swenson y Susana C. Lemozy, *Profesionalismo de inteligencia en las Américas*, op. cit. y *Democratización de la función de inteligencia*, op. cit.

313 Véase Nicolás Boscovich, “Pensamiento geopolítico brasileño”, en *Geopolítica* No. 34, 1986, Buenos Aires. También, más reciente, Lucas Figueiredo, *Ministério do silêncio* (São Paulo: Editora Record, 2005).

314 Particularmente la revista “Estrategia”, dirigida por el General Juan E. Gugliamelli.

315 Un buen ejemplo es la ley de inteligencia en Uruguay, aún en trámite parlamentario. La ley de defensa se aprobó hacia fines de 2008.

316 En este sentido, podemos citar a Carlos Repalli, *Inteligencia Criminal en el Siglo XXI* (Buenos Aires: Lajouane, 2009). Del mismo autor, *Inteligencia Criminal para la legislación de la Nación Argentina*, (Buenos Aires: Lajouane, 2007). También, en materia económica, Walter Felix Cardoso, *Guía de Inteligencia Empresarial: Enfrentando el ambiente de la alta competencia* (Buenos Aires: Seguridad y Defensa, 2006).

317 Thomas Bruneau, “Controlling Intelligence in New Democracies”, *International Journal of Intelligence and Counterintelligence* 14 no. 3, (otoño 2001), pp. 323-341.

318 Armando Borrero Mansilla ha explicado cuál es la lógica de los organismos de inteligencia que, con anuencia del gobierno o sin ella, esquivan o ignoran los mecanismos de control. De acuerdo a este intelectual colombiano, como la información es poder, el poder da seguridad y la seguridad da mejores posibilidades de supervivencia, la transparencia se invalida porque pone en peligro a la comunidad que se dice defender. Ver al respecto Armando Borrero Mansilla, “De Wikileaks a la trivialidad y al olvido: Reir, llorar...o rezar”, *Razón Pública*, 13 diciembre 2010.

319 “Temen crisis institucional en Brasil por escuchas ilegales”, *Infobae*, 1 septiembre 2008.

320 “Hijo de puta, no vuelva a este país”, *ABC (Madrid)*, 28 septiembre 2010.

321 “Cubanos realizan espionaje digital en Venezuela”, *Infolatam*, 16 junio 2011.

## Gestión de Inteligencia en las Américas

322 Véase “Los papeles secretos del DAS”, *Semana.com*, 17 septiembre 2011. Disponible en <http://www.semana.com/nacion/papeles-secretos-del-das/164304-3.aspx>. Consultado 7 abril 2012.

323 Véase en este sentido Mariano Bartolomé y Javier Ortíz: “Apuntes sobre la inteligencia en la Posguerra Fría”, *Seguridad Estratégica Regional* (SER) N° 8 (1995), pp. 71-79. También Mariano Bartolomé, “El Desafío de la inteligencia estratégica”, informe de investigación N° 1 (Buenos Aires: Instituto de Investigaciones sobre Seguridad y Crimen Organizado—ISCO, Universidad Católica de Salta, diciembre 1999).

324 Marco Cepik, *Espionagem e Democracia* (Rio de Janeiro: Editora FGV, 2003), pp. 27-28.

325 Cada uno de estos temas, a su vez, admite diferentes matices. Sólo por dar un ejemplo entre tantos posibles, en materia de control de las actividades de inteligencia por parte del congreso: ¿Lo hará una única comisión, o más de una? ¿Será una comisión bilateral, o se insertará en una de las cámaras legislativas? ¿Será una comisión creada con ese objeto, o la tarea la asumirá alguna comisión preexistente, como la que atiende las cuestiones de defensa? ¿Los organismos de inteligencia tienen la obligación de elevar informes periódicos a sus instancias de control, o solamente cuando se lo requieren?

326 El caso argentino muestra los dilemas que pueden presentarse en torno a la inteligencia estratégica: aunque doctrinariamente el concepto es empleado, la Ley 25520 que regula la actividad no lo menciona y la entrada en vigencia de ese instrumento legal implicó el cierre de la Central Nacional de Inteligencia (CNI) que llevaba a cabo esa tarea.

327 Merece mencionarse aquí la única actividad académica que el autor conoce sobre debates entre funcionarios de inteligencia, asesores parlamentarios y académicos sobre los contenidos y alcances de la inteligencia estratégica, sus características específicas y desafíos hacia el futuro. Adoptó la forma de un seminario titulado “La inteligencia estratégica en la reformulación del Estado”, se realizó durante buena parte del año 1992 en la Escuela Nacional de Inteligencia y su informe final fue publicada por la revista de esa institución. Ver “La inteligencia estratégica en la reformulación del Estado”, *Revista de la ENI* III:1 (Buenos Aires, 1994), pp. 143-152.

328 Desde una perspectiva constructivista, la “securitización” es un proceso discursivo y político mediante el cual una comunidad política decide tratar algo como una amenaza hacia un objeto de referencia valuado, habilitando la adopción de medidas urgentes y excepcionales para contrarrestar tal amenaza.

329 Ángel Tello, “La incertidumbre estratégica”, en Mariano Bartolomé (comp.), *Seguridad y defensa en tiempos de bicentenario: Visiones desde Argentina y Chile* (Buenos Aires: Instituto de Publicaciones Navales, 2010), pp. 21-34; Natalie Pabón Ayala, “Las relaciones cívico-militares en la política de seguridad democrática”, en Alejo Vargas Velásques (ed.), *Perspectivas actuales de la seguridad y la defensa en Colombia y América Latina*, Colección Gerardo Molina N° 15 (Bogotá: Universidad Nacional de Rosario, 2008), pp. 51-64.

330 “Senderistas se capitalizan en Bolivia”, *La Razón*, 7 marzo 2009; “Cómo funciona el mayor centro de venta de drogas”, *Clarín*, 18 abril 2010.

331 Consideramos verídicos los reportes emitidos por el gobierno colombiano respecto a la información contenida en las computadoras personales de Raúl Reyes, y también consideramos fiable la verificación efectuada por INTERPOL, cuyos detalles son públicos. Ver en este sentido OIPC-INTERPOL, *Informe forense de Interpol sobre los ordenadores y equipos informáticos de las FARC decomisados por Colombia* (Lyon: OIPC-INTERPOL, 2008).

332 Mariano Bartolomé, “Secuestros extorsivos y reivindicaciones campesinas: la rara alquimia del Ejército Popular Paraguayo”, *Analítica*, 5 mayo 2010. Disponible en <http://www.analitica.com/val/internacionales/opinion/3857731.asp>. Consultado 11 abril 2012.

333 Cifras emitidas por el Secretario General de la esa organización, José Miguel Insulza en julio de 2009, en su intervención en la *Conferencia Interamericana de Seguridad Pública* celebrada en Montevideo. En Mariano Bartolomé, “Situación del crimen organizado en América Latina”, *Ágora Internacional*, N° 10 (noviembre 2009), pp. 16-20.

334 El reporte también indica que 5 de las 10 ciudades más violentas del mundo son mexicanas; 45 de las 50 ciudades más violentas se sitúan en el continente americano y 40 en América Latina; la jurisdicción subnacional más violenta del mundo corresponde a Honduras y 3 de las 10 jurisdicciones subnacionales más violentas del mundo son hondureñas; y que 19 de las 50 jurisdicciones nacionales más violentas del mundo se ubican en México y en Centroamérica. Para mayores datos, ver *Consejo Ciudadano para la Seguridad Pública y la Justicia Penal: Metodología del ranking (2011) de las 50 ciudades y las 50 jurisdicciones subnacionales más violentas del mundo* (México, DF, 12 enero 2012).

335 United Nations Office on Drugs and Crime, *World Drug Report* (Vienna: UNODC, 2011), pp. 85-126.

## Gestión de Inteligencia en las Américas

336 Mariano Bartolomé, “Colombia: Bandas Criminales (BACRIM)”, *Reconciliando Mundos*, N° 7, (septiembre-octubre 2011), pp. 16-22.

337 Rachel Stohl y Doug Tuttle, “The Small Arms Trade in Latin America,” *NAC-LA Report on the Americas* 41, N° 2 (marzo-abril 2008), p. 14. También Fernando Gualdoni y Javier Lafuente, “Las armas ilegales desangran Latinoamérica”, *El País*, 25 mayo 2009.

338 “Tráfico de armas en los Andes”, *El Universal*, 27 abril 2008.

339 Grupo de Estudiantes de Relaciones Internacionales de la Universidad de Palermo (GERIUP), “Tráfico de personas en América del Sur”, *Informes del GERIUP*, 19 octubre 2011.

340 En este punto, el aspecto preventivo resulta fundamental. Alega un informe del Banco Internacional de Desarrollo (BID) (véase <http://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=876738>) que una adecuada inversión en prevención reduce entre seis y siete veces las sumas que se deben erogar para lidiar ex post con los efectos de la amenaza, una vez consumada. De Jorge Serrano Torres, *Las potencialidades de una doctrina y un sistema de inteligencia criminal para desarticular al crimen organizado y afianzar la seguridad ciudadana en el Perú*, (Lima: Projusticia-Centro de Estudios para el Desarrollo de la Justicia, noviembre 2011). Personalmente consideramos que en algunas cuestiones puntuales como el terrorismo, la reducción puede ser aun mayor.

341 Carlos Gutiérrez Palacios, “El papel de la inteligencia estratégica ante los desafíos regionales”, *Revista Atenea*, 6 octubre 2010.

342 “Narcotráfico debe verse como una amenaza para toda la región, dijo el jefe de inteligencia brasileña”, *El Tiempo*, 13 agosto 2009.

343 “Forman a militares para combatir al EPP”, *ABC Color*, 1 marzo 2011; “Defensa tendrá más poder sobre las fuerzas armadas, reconoce el ministro”, *ABC Color*, 3 marzo 2011.

344 “Claves de la reforma de las fuerzas armadas”, *La República*, 7 marzo 2011.

345 “Video: Colman (DNII) duda de la existencia de un ejército paralelo”, *La Red 21*, 17 marzo 2011.

346 Ver en este sentido Luis Casal Beck, “Una inteligencia segmentada”, *La Red 21*, 1 abril 2011.

347 “El DAS deja de existir para dar paso a la Agencia Nacional de Inteligencia”, *Semana.com*, 31 octubre 2011. Para una buena recopilación de los antecedentes de disolución del DAS, los diferentes proyectos de ley que abordaron su reemplazo y otras cuestiones vinculadas, ver “Agencia Central de Inteligencia de Colombia”, *Observatorio Legislativo del Instituto de Ciencia Política*, Boletín N° 144 (noviembre 2009).

348 Serrano Torres, *op. cit.*

349 Un pormenorizado detalle de esta operación en “Así cayó Raúl Reyes”, *Cambio*, 12 marzo 2008.

350 María Amparo Tortosa Garrigós, “Cómo se están redefiniendo las agencias de inteligencia: Las nuevas amenazas y conflictos requieren de un nuevo tipo de cooperación”, *Safe Democracy*, 12 enero 2009.

351 Roger Zane George, “Beyond Analytic Tradecraft”, *International Journal of Intelligence and CounterIntelligence* 23, no. 2 (June 2010).

352 La especialista chilena Carolina Sancho propone una interpretación diferente sobre las características de un sistema o una comunidad de inteligencia. Mientras el primer concepto se circunscribe a la interacción entre los organismos de inteligencia, el segundo incluye diversos organismos públicos, y cada uno de ellos tiene un aporte sustantivo y sistemático que realizar en temas de interés estratégico para el país. En Carolina Sancho Hirane, “Servicios de Inteligencia en las Américas: Estado del debate y desafíos pendientes”, en Mariano Bartolomé (comp.), *Seguridad y defensa en tiempos de bicentenario: Visiones desde Argentina y Chile* (Buenos Aires: Instituto de Publicaciones Navales, 2010), pp. 149-168.

353 “Mujica no aceptó la renuncia de Grégori, el Coordinador Nacional de Inteligencia”, *La Red 21*, 1 abril 2011.

354 “Comando conjunto de fuerzas armadas asumió control del Sistema de Inteligencia”, *El Universo*, 18 octubre 2010.

355 “Colombia: Santos crea la figura del Consejero de Seguridad Nacional”, *Infolatam*, 20 septiembre 2010.

356 Félix Arteaga, “Una década de cambios en la seguridad tras el 11-S: de la globalización a la glocalización”, *Real Instituto Elcano, ARI* 125/2011, 6 septiembre 2011.

## Gestión de Inteligencia en las Américas

357 Oficina de las Naciones Unidas, *Un mundo más seguro: la responsabilidad que compartimos*. Informe del Grupo de Alto Nivel sobre las amenazas, los desafíos y el cambio, A/59/565, 2 diciembre 2004. Disponible en [http://www.un.org/spanish/secureworld/report\\_sp.pdf](http://www.un.org/spanish/secureworld/report_sp.pdf). Consultado 7 abril 2012.

358 “Sendero Luminoso es hoy un museo de cera del terrorismo que había en el Perú”, *El Comercio*, 7 septiembre 2010.

359 “Zares antidrogas buscan combatir lavado de activos del narcotráfico”, *El Nuevo Herald*, 5 octubre 2010.

360 Mario Baizán, “Cooperación internacional en la zona de la Triple Frontera”, *mimeo* (Buenos Aires: Fundación de Estudios Políticos para el Tercer Milenio – FUPOMI, 2004). Disponible en <http://www.fupomi.com.ar/img/TripleF.pdf>. Consultado 7 abril 2012.

361 La información pública sobre estas unidades de coordinación es escasa, y más aún en formatos académicos. Entre las pocas fuentes disponibles, se propone Ramón Quiroga, “Políticas de seguridad y defensa en América del Sur”, ponencia expuesta en el V Encuentro Nacional de Estudios Estratégicos, Buenos Aires, octubre 2002.

362 Pablo Martínez, *Triple Frontera: un modelo de cooperación antiterrorista* (Montevideo: Centro de Estudios Hemisféricos de Defensa (CHDS), Conferencia Subregional de Defensa “Seguridad Transnacional y Gobernabilidad”, noviembre 2005).

363 La Comunidad Latinoamericana y del Caribe de Inteligencia Policial fue creada en el año 2005, con el objetivo de capacitar personal de inteligencia y facilitar el intercambio de información entre las partes. Hoy está integrada por casi treinta países, además de cuatro observadores externos: la ONU, la Organización de Estados Americanos (OEA), EUROPOL y España, representado por el Centro Nacional de Inteligencia (CNI) español.

364 “México compartirá su plataforma de inteligencia con América Latina y el Caribe”, *Agencia EFE*, 3 julio 2010.

365 Richard Kugler, *Policy Analysis in National Security Affairs: New Methods for a New Era* (Washington, DC: National Defense University Press, 2006), pp. 37-38.

366 El empleo de analogías históricas es un recurso válido en los análisis de política internacional contemporánea, como en inteligencia estratégica. Sin embargo, no son válidas las perspectivas que sostienen que todo fenómeno internacional relevante de la actualidad es análogo a algún caso histórico, sin excepción. Un ejemplo

de esta lectura se observa en Robert Kaplan, *El retorno de la antigüeda: La política de los guerreros* (Barcelona: Editorial B, 2002).

367 Existen numerosas referencias a la importancia de estas áreas de conocimiento en el análisis estratégico actual. A modo de ejemplo, véanse Bjørn Moller, “Ethnic Conflict and Postmodern Warfare: What is the Problem? What could be done?”, COPRI, Working Paper, October 1996; Eric de la Maissonave, *Incitation à la Reflexion Stratégique* (Paris: Economica, 1998); Alain Joxe, *El Imperio del Caos* (Buenos Aires: Fondo de Cultura Económica, 2003); y United States Army, *Counterinsurgency Field Manual* (Chicago: The University of Chicago Press, 2007).

368 “Colombia ya cuenta con un nuevo material estadístico del Sector de la Defensa y la Seguridad”, *Infodefensa.Com*, 7 septiembre 2010.

369 Aquí entendemos a los escenarios en la forma en que los conceptúa el Saint Gall Center for Futures Research: “imágenes del futuro, que representan un proceso, están basados en una metodología, incorporan el conocimiento de expertos y facilitan el aprendizaje organizacional”.

370 George Friedman, *The Next 100 Years. A Forecast for the 21st Century* (New York: Anchor Books, 2010).

371 National Intelligence Council, *Global Trends 2015: A Transformed World* (Washington, DC: U.S. Government Printing Office, noviembre 2008).

372 José Miguel Pizarro, “América Latina: la guerra que ya no podemos evitar”, *Revista AAInteligencia* 2010-3. Véase <http://www.aainteligencia.cl>.

373 Rogelio Nuñez, “Sendero Luminoso: de guerra maoísta a cártel”, *Revista Atenea*, 14 febrero 2011.

374 El CDS constituye una arquitectura de seguridad regional que comenzó a ser elaborada por los doce países de la Unión de Naciones Sudamericanas (UNASUR) luego de la crisis desatada por el ataque militar colombiano a un campamento de las FARC ubicado en territorio ecuatoriano, en marzo del año 2008. Su institucionalización tuvo lugar en Santiago de Chile en marzo de 2009 y en el documento fundacional, titulado *Declaración de Santiago de Chile* las partes acordaron construir una identidad propia de América del Sur en esta materia, que tome en cuenta las características subregionales y nacionales, y que contribuya al fortalecimiento de la unidad de América Latina y el Caribe.

## Gestión de Inteligencia en las Américas

375 Se agradecen los aportes gráficos de Andrés González Vargas (GOVA), catedrático de la Universidad Jorge Tadeo Lozano de Bogotá y el estímulo de Ámparo Vásquez Gallo, esposa del autor.

376 Gregory Treverton, "Intelligence and the 'Market State'", *Studies in Intelligence* 10 (Winter/Spring 2001), p. 71.

377 Pierre Lacoste, *Una nueva estrategia para la inteligencia* (Buenos Aires: Escuela Nacional de Inteligencia, 1999), p. 8. El primero mundo es el oficial, el de los Estados soberanos responsables, miembros de la Organización de las Naciones Unidas, que están obligados a aceptar las reglas y los códigos de conducta del derecho internacional.

378 Ver Moisés Naím, *Ilícito: Cómo traficantes, contrabandistas y piratas están cambiando el mundo* (México: Random House Mondadori, 2007).

379 Carlos Lleras Restrepo, "Los escándalos financieros", *Revista Nueva Frontera* (Bogotá), julio de 1988.

380 Pilar Pozo Serrano, "Externalización de funciones de inteligencia: oportunidades y riesgos a la luz de la experiencia estadounidense", *Inteligencia y Seguridad: Revista de análisis y prospectiva*, N.º. 6 (junio-noviembre 2009), p 19. Disponible en [www.uv.es/~pozop/externalizacioninteligencia.pdf](http://www.uv.es/~pozop/externalizacioninteligencia.pdf). Recuperado 1 diciembre 2014.

381 "Espionaje. El que indebidamente obtenga, emplee o revele secreto político, económico o militar relacionado con la seguridad del Estado, incurrirá en prisión de cuatro (4) a doce (12) años". Código Penal Ley 599 de 2000. Título XVII: Delitos contra la existencia y seguridad del Estado, capítulo II, artículo 463.

382 "La configuración de un derecho penal del enemigo se hace patente en las legislaciones penales contemporáneas con independencia de si puede considerarse legítima o no. La constatación de este dato, aunque produzca en algunos un fuerte rechazo, no puede negarse. En la legislación penal peruana puede apreciarse con facilidad esta orientación de la regulación penal en el caso de los delitos de terrorismo, narcotráfico, criminalidad organizada, violación sexual de menores de edad y corrupción de funcionarios... Los delitos económicos no han adquirido todavía el rechazo social que posiblemente si ha alcanzado en Europa y, por lo tanto, no se ha desarrollado un derecho penal del enemigo para los delincuentes económicos". Percy García Cavero, *Derecho Penal Económico*, Tomo I (Lima: Editorial Jurídica Grijley, 2007), pp. 103 y 105.



383 Afirmó el presidente venezolano Hugo Chávez: “La Dirección de los Servicios de Inteligencia y Prevención (Disip), ahora Servicio Bolivariano de Inteligencia Nacional (Sebin), organismo que en el pasado era un cuerpo represivo, de choque. Los funcionarios andaban en la calle con motos, ‘chapeando’, atemorizando, pero ese organismo es para hacer inteligencia económica, internacional, inteligencia de Estado”. “PNB [Policía Nacional Bolivariana] cuenta con 2.426 funcionarios en sus primeros seis meses de funcionamiento”. Agencia Venezolana de Noticias, 20 julio 2010. Disponible en: <http://www.avn.info.ve/node/5988>. Recuperado 20 julio 2011.

384 Se puede deducir que no existe una política de Estado y un plan estratégico como país para prevenir el lavado de activos, ni para combatir el financiamiento del terrorismo. En 2010, el Grupo de Acción Financiera Internacional incluyó a Ecuador en la lista negra de países sin leyes contra el lavado de dinero. Ver *Eldiario.ec* 18 febrero 2010, en <http://www.eldiario.com.ec/noticias-manabi-ecuador/144026-incluyen-a-ecuador-en-lista-negra-de-lavado-de-dinero/>. También Patricio X. Sánchez, Ramiro Crespo Fabara y Patricio Starnfeld Llamazares, “Prevención de lavado de activos frente a la concienciación: Conferencia sobre lavado de activos y financiamiento del terrorismo”, en *Inteligencia Estratégica y Prospectiva*, coordinador Fredy Rivera Vélez *op. cit.*, pp. 239-264.

385 Andrés Montero Gómez y José Martín Ramírez, “Inteligencia económica como vector internacional de seguridad”, *Real Instituto Elcano*, 21 abril 2008. Disponible en: [http://www.realinstitutoelcano.org/wps/portal/riecano/contenido?WCM\\_GLOBAL\\_CONTEXT=/elcano/elcano\\_es/zonas\\_es/defensa+y+seguridad/dt18-2008](http://www.realinstitutoelcano.org/wps/portal/riecano/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/defensa+y+seguridad/dt18-2008). Recuperado 8 enero 2011.

386 Ohad Leslau, “Intelligence and Economics: Two Disciplines with a Common Dilemma”, *International Journal of Intelligence and Counterintelligence* 20, no. 1 (2007), p 106.

387 “Aquellos que sólo pueden mostrar el título de primer nivel de educación superior (‘economista’) no son contratados para hacer el diagnóstico y tratamiento de las principales ‘enfermedades económicas’ del país... Para alcanzar ese nivel hay que acumular más capital educativo haciendo un Ph.D, preferentemente en los Estados Unidos ... Lo que podemos comprobar es la proliferación de Facultades de Economía, la masificación de los graduados y su marginación de los centros de toma de decisiones”. Marco Palacios, “Saber es poder: el caso de los economistas colombianos”, en *De populistas, mandarines y violencias, luchas por el poder* (Bogotá: Editorial Planeta, 2001), pp. 119 y 134.

## Gestión de Inteligencia en las Américas

388 “Esta teoría de inteligencia tiene como propósito explicar por qué los Estados van a la guerra cuando los cálculos de su poder sugieren que ellos perderán y porque algunos Estados ganan contiendas a pesar de ser militarmente inferiores”. Jennifer Sims, “Defending Adaptive Realism: Intelligence Theory Comes of Age”, en *Intelligence Theory: Key questions and Debates*, ed. Peter Gill, Stephen Marrin, y Mark Phythian (London & New York: Routledge, 2009), p. 154.

389 Sims, *ibid*, p. 154.

390 “Refinería de Cartagena y ducto serían viables”, *Petróleo y Gas*, 8 noviembre 2005. Disponible en: [http://www.bnamericas.com/news/petroleoygas/Refineria\\_de\\_Cartagena\\_y\\_ducto\\_serian\\_viables](http://www.bnamericas.com/news/petroleoygas/Refineria_de_Cartagena_y_ducto_serian_viables). Recuperado 28 septiembre 2011.

391 “Rubens Ferreira de Mello escribe en su Tratado de Derecho Diplomático: Entre las acusaciones que se hacen a la diplomacia, una de las más frecuentes es la que se refiere al papel, no siempre confesable, representado por ella en ciertas épocas de la historia, al servicio de gobiernos poco escrupulosos, autorizando cuestiones de prestigio o de hegemonía. Esa manera de proceder es conocida con el nombre de diplomacia secreta (...) Lo cierto es que fines de prestigio e intentos hegemónicos han merodeado en muchos de los gabinetes donde se maneja la política exterior, y no pocas veces se han traducido en instrucciones precisas y concretas a los agentes plenipotenciarios”. Diego Uribe Vargas, *Colombia y la Diplomacia Secreta* (Bogotá: Universidad Jorge Tadeo Lozano y Academia Colombiana de Historia, 2005), pp. 28 y 29.

392 “Inversiones de Chávez en el país son peligrosas: ex ministro Santos”, *El Colombiano.com*, 8 noviembre 2005. Disponible en: [http://www.elcolombiano.com/BancoConocimiento/Ol/olac\\_santos\\_se\\_refiere\\_a\\_interes\\_de\\_chavez\\_colprensa\\_lcg\\_08112005/olac\\_santos\\_se\\_refiere\\_a\\_interes\\_de\\_chavez\\_colprensa\\_lcg\\_08112005.asp](http://www.elcolombiano.com/BancoConocimiento/Ol/olac_santos_se_refiere_a_interes_de_chavez_colprensa_lcg_08112005/olac_santos_se_refiere_a_interes_de_chavez_colprensa_lcg_08112005.asp). Recuperado 12 diciembre 2010.

393 Claudia Curiel Leidenz, “La economía durante la Revolución Bolivariana”, en *Hugo Chávez: una década en el poder* (Bogotá: Centro de estudios Políticos e Internacionales, Universidad del Rosario, 2010), p. 414.

394 Moisés Naím, *op. cit.*, p. 55.

395 *Ibid*, p. 24.

396 “Hay mucho contrabando ilegal a lo largo de la frontera entre Colombia y Venezuela que involucra drogas, gasolina y automóviles. Si bien la región de la frontera tripartita, donde se encuentran Brasil, Paraguay y Argentina, es más conocida

como concentradora de contrabando en América Latina, la frontera entre Colombia y Venezuela es quizás aún más porosa y canaliza vastas cantidades de cocaína y otros productos básicos... Y si bien no tienen [las bandas criminales] una agenda nacional como los líderes de las AUC (Autodefensas Unidas de Colombia), entienden que su poder crece y las empresas criminales prosperan siempre que tengan buenas conexiones con los políticos locales”. Vanda Felbab-Brown, *Las economías ilegales y el contrabando en Colombia: Los señores de las moscas* (Washington, DC: Brookings Institution, 21<sup>st</sup> Century Defense Initiative), 22 febrero 2011. Disponible en [http://www.brookings.edu/opinions/2011/0222\\_colombia\\_felbabbrown.aspx?sc\\_lang=es](http://www.brookings.edu/opinions/2011/0222_colombia_felbabbrown.aspx?sc_lang=es). Recuperado 28 septiembre 2011.

397 William J. Bernstein, *A Splendid Exchange, How trade Shaped the World* (New York: Atlantic Monthly Press, 2008), p. 376.

398 “Hay varias razones para creer que las fuerzas armadas de Venezuela no son tan pro-bélicas como Chávez lo quisiera, una clave es que las fuerzas armadas son las mayores beneficiarias del comercio lícito e ilícito con Colombia y los EE.UU.” Javier Corrales, “Cambios en el tipo de régimen y la nueva política exterior de Venezuela”, en *Hugo Chávez: una década en el poder, op. cit.*, p. 477.

399 Tal aseveración surge a raíz de la intuición y experiencia profesional del autor.

400 Sims, *op. cit.*, p. 62.

401 Alocución Presidencial del 17 noviembre 2008. Disponible en [http://web.presidencia.gov.co/boletin/boletin\\_no2\\_17112008.html](http://web.presidencia.gov.co/boletin/boletin_no2_17112008.html). Recuperado 05 marzo 2009.

402 “Las Farc también ‘invirtieron’ en DMG”, *Revista Semana*, 19 febrero 2010. Disponible en: <http://www.semana.com/nacion/farc-tambien-invirtieron-dmg/135207-3.aspx>. Recuperado 22 septiembre 2011.

403 “Gobernador de Putumayo: las Farc estarían aprovechando crisis por las pirámides para poner al pueblo contra el gobierno”, *Radio Caracol*, 2 diciembre 2008. Disponible en: <http://www.caracol.com.co/nota.aspx?id=722564>. Recuperado 5 marzo 2009.

404 “A responder por pirámides”, *El Espectador.com*, 24 noviembre 2008. Disponible en: <http://www.elespectador.com/impreso/articuloimpreso93236-responder-piramides>. Recuperado 5 marzo 2009.

## Gestión de Inteligencia en las Américas

405 “En el caso de las pirámides, ‘faltó gobierno”, *El Espectador.com*, 15 noviembre 2008. Disponible en: <http://m.elespectador.com/impreso/cuadernilloa/entrevista-de-cecilia-orozco/articuloimpreso90777-el-caso-de-piramides-falto-go>. Recuperado 5 marzo 2009.

406 “¿Quién espía en Colombia?”, Informe especial, *Semana.com*, 21 julio 2003. Disponible en: <http://www.semana.com/nacion/quien-espia-colombia/71742-3.aspx>. Recuperado 18 noviembre 2010.

407 “Las revelaciones de Tabares y Peñate”. *El Espectador.com*, 1 enero 2011 Disponible en: <http://www.elespectador.com/impreso/judicial/articulo-242994-revelaciones-de-tabares-y-penate>. Recuperado 18 enero 2011.

408 Sims, *op. cit.*, p. 156.

409 “En el caso de los exportadores colombianos, cuando Chávez cerró la frontera comercial a mediados de 2009, había una deuda de los venezolanos con ellos cercana a US\$900 millones. El cierre de la frontera comercial fue acompañado de un acto igualmente hostil: el no otorgamiento de divisas para el pago de las exportaciones ya efectuadas”. Disponible en <http://lanota.com/index.php/CONFIDENCIAS/Venezuela-no-le-paga-a-los-exportadores-colombianos.html>. Recuperado 09 diciembre 2011.

410 “Desde el punto de vista de la política comercial, además, con la posición crítica del gobierno de Chávez hacia el ALCA (Área de Libre Comercio de las Américas) se había hecho imposible que Colombia y Venezuela tuvieran una misma posición en las negociaciones hemisféricas. La coordinación era muy difícil, según Javier Díaz, presidente de Analdex, y eso ahora va a mejorar: Carmona es un convencido en el libre comercio”. Véase “Colombia: bien librada”, *El Tiempo*, 14 abril 2002. Disponible en: <http://www.eltiempo.com/archivo/documento/MAM-1384048>. Recuperado 05 junio 2011. “Una carta enviada por el presidente de la Andi, Luis Carlos Villegas, al entonces presidente de Fedecámaras y por algunas horas presidente de Venezuela, Pedro Carmona, se convirtió en la manzana de la discordia del gobierno de Hugo Chávez con una parte del empresariado colombiano”. En “Empresarios descontentos”, *El Tiempo*, 8 julio 2003. Disponible en <http://www.eltiempo.com/archivo/documento/MAM-1014926>. Recuperado 5 junio 2011.

411 “El gobierno [ecuatoriano] “argumenta que existió aproximadamente un 40 por ciento de devaluación” del peso colombiano, mientras que, según las cifras que maneja la Cámara de Comercio ecuatoriana-colombiana, “técnicamente no

se ha dado esa devaluación”, dijo el presidente de la institución, Milton Delgado”. Ecuador pone en vigencia “salvaguardia cambiaria” contra Colombia. Disponible en <http://spanish.peopledaily.com.cn/31617/6699818.html>. Recuperado 12 enero 2012.

412 Alphonso Chardy, “Chavez Expanding Influence of Cuban Advisers,” *Miami Herald*, 8 mayo 2004.

413 “La tenaza cubana,” *Semana.com*, 13 February 2010. Disponible en <http://www.semana.com/mundo/tenaza-cubana/134903-3.aspx>. Consultado 12 enero 2012.

414 Un pueblo sin memoria y malagradecido, *Eluniversal.com* (Caracas), 18 junio 2011. Disponible en <http://www.eluniversal.com/2011/06/18/un-pueblo-sin-memoria-y-malagradecido.shtml>. Recuperado 13 septiembre 2011.

415 “Juego de espías”, *Semana.com*, 25 agosto 2007. Disponible en <http://www.semana.com/nacion/juego-espias/105816-3.aspx>. Recuperado 3 septiembre 2011.

416 “El chavismo estaría financiando políticos en el territorio nacional. Renuncias en Monómeros por supuesta actividad chavista en Colombia”, *Elespectador.com*, 14 agosto 2008. Disponible en <http://www.elespectador.com/impreso/politica/articulo-impreso-renuncias-monomeros-supuesta-actividad-chavista-colombia>. Recuperado 25 septiembre 2011.

417 Sgto. Salazar Evelio Buitrago, *Zarpazo, otra cara de la violencia: Memorias de un suboficial del ejército de Colombia* (Bogotá: Ministerio de Defensa, 1968), p. 169.

418 Constitución Nacional, artículo 2. “Son fines esenciales del Estado: servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo. Las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares”.

419 “EE.UU. asume la protección del petróleo colombiano”, *El Clarín*, 11 febrero 2002. Disponible en <http://edant.clarin.com/diario/2002/02/11/i-02415.htm>. Recuperado 28 septiembre 2011.

## Gestión de Inteligencia en las Américas

420 Ver <http://www.egmontgroup.org/>.

421 Unidad de Información y Análisis Financiero, República de Colombia, *Descripción de cargos, funciones y perfiles*, sin fecha. Disponible en <http://www.uiaf.gov.co/index.php?idcategoria=677>. Recuperado 13 agosto 2011.

422 Proyecto de Ley Estatutaria N° 195 de 2011, artículo 3. – Organismos que llevan a cabo la función de inteligencia y contrainteligencia. La función de inteligencia y contrainteligencia es llevada a cabo por las dependencias de las fuerzas militares y la Policía Nacional organizadas por éstas para tal fin, la Unidad de Información y Análisis Financiero (UIAF), y por los demás organismos que faculte para ello la Ley. Estos organismos conforman la comunidad de inteligencia y son los únicos autorizados para desarrollar actividades de inteligencia y contrainteligencia. Todos los organismos que lleven a cabo estas actividades estarán sujetos al cumplimiento de la presente ley de manera integral.

423 “Política de Consolidación de la Seguridad Democrática: Fortalecimiento de las Capacidades del Sector Defensa y Seguridad”.

424 Constitución Nacional, artículo 339. “Habrá un Plan Nacional de Desarrollo conformado por una parte general y un plan de inversiones de las entidades públicas del orden nacional. En la parte general se señalarán los propósitos y objetivos nacionales de largo plazo, las metas y prioridades de la acción estatal a mediano plazo y las estrategias y orientaciones generales de la política económica, social y ambiental que serán adoptadas por el Gobierno....”.

425 Clara Elvira Ospina, “¿Inteligencia o intimididad?”, *Revista Poder360*, 18 septiembre 2010. Disponible en [http://www.poder360.com/article\\_detail.php?id\\_article=4755](http://www.poder360.com/article_detail.php?id_article=4755). Recuperado 12 febrero 2011.

426 Tal como la gama de pasos tomados por los EE.UU., documentado por Alain Juillet en “Principios y Aplicación de la Inteligencia Económica”, *Inteligencia y seguridad: Revista de análisis y prospectiva*, N° 1 (Diciembre 2006), p. 15. Disponible en [http://www.intelligence-economique.gouv.fr/IMG/pdf/Article\\_Alain\\_Juillet\\_pour\\_revue\\_espagnole.pdf](http://www.intelligence-economique.gouv.fr/IMG/pdf/Article_Alain_Juillet_pour_revue_espagnole.pdf). Recuperado 30 mayo 2011.

427 Según Naím, *op. cit.*, p. 55, el terrorismo internacional, por lo que empezamos a saber, sigue los pasos del comercio ilícito mundial y emplea los mismos instrumentos y servicios de la nueva economía global para difuminarse, y así ocultarse, en las ciudades y los países.

428 Edward Luttwak, "From Geo-Politics to Geo-Economics", *The National Interest* 20, no. 3 (verano 1990), p. 17.

429 Nicolás Urrutia, "Colombia necesita espías", *Semana.com*, 11 marzo 2009. Disponible en <http://www.semana.com/opinion/colombia-necesita-espias/121626-3.aspx>. Recuperado 11 junio 2009.

430 Marta Ardila, *Actores no Gubernamentales y Política Exterior* (Bogotá: Centro de Estudios Internacionales, Universidad de los Andes, 2009), p. 115.

431 Martin Nowak, *Supercooperadores* (España: Grupo Zeta, 2012), p. 55.

432 Sonia Alda y Héctor Saint-Pierre, (coords.), *Gobernabilidad y democracia* (Chile: RIL / UNESP / IUGM, 2012), p. 219.

433 Se destaca que en el marco de UNASUR no hay formalmente un mecanismo de cooperación en inteligencia. Todos los países soberanos del continente de Suramérica son miembros de UNASUR.

434 Forma parte del proyecto de investigación de ANEPE extramuro código n° ext/12/2012, desarrollado por la autora, durante el período 2012 – 2013, titulado "Cooperación en Inteligencia y UNASUR: Posibilidades y Limitaciones". Se agradece la colaboración del cientista político Jean Gutiérrez.

435 Julia Pulido, "El papel de la Inteligencia en la PESD (Política Europea de Seguridad y Defensa)", *Cuadernos de Estrategia* (Ministerio de Defensa de España) N° 130, 2005; Robert Clark, *Intelligence Analysis*, segunda edición (Washington, DC: CQ Press, 2007); Antonio Díaz Fernández, (coord.), Miguel Revenga y Oscar Jaime, *Cooperación Europea en Inteligencia* (España: Thomson Reuters y IUGM, 2009).

436 Mathieu Deflem, "Global Rule of Law or Global Rule of Law Enforcement? International Police Cooperation and Counterterrorism", *Anuario de la American Academy of Political and Social Science*, vol. 603, *Law, Society, and Democracy: Comparative Perspectives*, (enero 2006), pp. 240-251.

437 Rhodri Jeffreys-Jones, *Historia de los Servicios Secretos Norteamericanos* (España: Editorial Paidós, 2004), p. 32.

438 Inge Kaul y otros, *Bienes Públicos Mundiales* (México: Oxford, 2001).

439 Peter Bergen y Alec Reynolds, "De nuevo, la contraofensiva a las acciones occidentales", *Revista Foreign Affairs en Español*, vol. 84, N° 6 (enero-marzo 2006). Publicado por el Instituto Tecnológico Autónomo de México, México.

## Gestión de Inteligencia en las Américas

440 Hans Blix, ¿*Desarmando a Irak?* (España: Planeta, 2004).

441 Al respecto ver Eduardo Aldunate, *Misión en Haití* (Chile: Centro de Estudios Bicentenario, 2007); Eduardo Aldunate, *Las razones políticas y morales de la misión ONU en Haití* (España: FRIDE, 2008). Disponible en [http://www.fride.org/download/COM\\_UN\\_Haiti\\_ESP\\_abr08.pdf](http://www.fride.org/download/COM_UN_Haiti_ESP_abr08.pdf).

442 Melanie Ramjoue, "Improving United Nations Intelligence: Lessons from the Field", GCSP Policy Paper no. 19 (agosto 2011), Geneva Centre for Security Policy. Disponible en <http://www.gcsp.ch/content/download/6457/59721/download>.

443 Julia Pulido, op. cit.; Antonio Díaz, Miguel Revenga, Oscar Jaime, y Rafael Martínez. "Hacia una política europea de inteligencia", *Revista Política Exterior* (España), vol. XIX, N° 106 (agosto 2005).

444 Estatuto de Consejo de Defensa Suramericano, artículo 5, letra B, *Consejo de Defensa Suramericano: Crónica de su gestión* (Chile: Ministerio Defensa Nacional, 2009), p. 169. Documento obtenido del Grupo de Trabajo del Consejo de Defensa Suramericano.

445 José Manuel Ugarte, "El Consejo de Defensa Suramericano: Naturaleza, balance provisorio, perspectivas y desafíos", en Hans Mathieu y Catalina Niño (eds.), *Anuario 2010 de la Seguridad Regional en América Latina y el Caribe* (Colombia: Friedrich Ebert Stiftung, 2010), p. 34.

446 Julia Pulido, op. cit., p. 288.

447 Andrés Gómez de la Torre, "Intereses académicos compartidos: hacia una comunidad iberoamericana de inteligencia", *Inteligencia y Seguridad: Revista de Análisis y Prospectiva*, N° 2. Universidad Rey Juan Carlos, España (Cátedra Servicios de Inteligencia y Sistemas democráticos) y Universidad Carlos III de Madrid (Instituto Juan Velásquez de Velasco de Investigación para la Seguridad y Defensa), 2007.

448 Andrea Carvalho y Miguel Esteban, "Los servicios de inteligencia: entorno y tendencias", en José González (coord.), *Inteligencia* (España: Tirant lo Blanch, 2012), p. 92.

449 José Manuel Ugarte, "Aportes y propuestas para la cooperación de Inteligencia", *Revista Política y Estrategia* (ANEPE) N° 120 (julio-diciembre 2012), p. 163.

450 Para efectos de esta parte del trabajo se han considerado los aportes de Antonio Díaz, (coord.), Miguel Revenga, y Oscar Jaime, op. cit., y José Manuel Ugarte, "Aportes y propuestas para la cooperación de Inteligencia" op. cit.



451 José Manuel Ugarte, “Aportes y propuestas para la cooperación de inteligencia”, *op. cit.*, p. 161.

452 *Ibid.*, p. 161.

453 *Ibid.*, p. 161.

454 En este tema hay diversas denominaciones para hacer referencia a la inteligencia orientada al delito y la prevención de situaciones que pueden afectar seriamente la seguridad pública. En este sentido podemos encontrar denominaciones como inteligencia policial, inteligencia criminal e información policial y hacen referencia al mismo objeto de estudio con variaciones en la amplitud de concepto, como en los organismos involucrados. En UNASUR, son las policías las encargadas de la inteligencia policial y es más característicos de España hablar de servicios de información policial, término ocupado en esta clasificación, referido a que ha sido extraída de un texto cuyos autores son españoles. Asimismo, cabe consignar que algunos autores –y también en algunos países– distinguen la inteligencia policial y la inteligencia criminal.

455 Antonio Díaz, (coord.), Miguel Revenga, y Oscar Jaime, *op. cit.*, p. 25.

456 *Ibid.*, p. 62.

457 José Manuel Ugarte, “Aportes y propuestas para la cooperación de Inteligencia”, *op. cit.*, p. 190.

458 MERCOSUR está integrado por Argentina, Brasil, Paraguay (suspendido), Uruguay, Venezuela y Bolivia (en proceso de adhesión). Asociados a este organismo son Chile, Colombia, Perú, Ecuador, Guyana (en proceso de ratificación) y Surinam (en proceso de ratificación). Cuando se indica MERCOSUR ampliado, se hace referencia a los integrantes de este organismo junto con sus miembros asociados.

459 Véase Celina B. Realuyo, “Collaborating to Combat Illicit Networks Through Interagency and International Effort”, capítulo 14 de Michael Miklaucic y Jaqueline Brewer, *Convergence: Illicit Networks and National Security in the Age of Globalization* (Washington, DC: National Defense University, 2013). Disponible en <http://www.ndu.edu/press/convergence.html>. Consultado 13 abril 2013.

460 Antonio Díaz Fernández, “Modelos de servicios de inteligencia en Europa y Latinoamérica”, en Rafael Martínez y Joseph Tulchin, *El Rompecabezas: Conformando la seguridad desde las dos orillas* (España: Centre d’Informació i Documentació Internacionals a Barcelona-CIDOB, 2006), p. 14.

## Gestión de Inteligencia en las Américas

461 Tim Schumacher, *Europas Geheimdienst: Das Joint Situation Centre*, 2011. Disponible en <http://www.imi-online.de/2011/06/02/europas-geheimdienst/>. Consultado 15 febrero 2013.

462 Hans-Georg Wieck, Multilaterale Zusammenarbeit der Geheimen Nachrichtendienste im Nordatlantischen Bündnis (NATO) – Ein Modell für die Europäische Union?, p. 1. Disponible en [http://www.hans-georgwieck.com/data/Eu%E4ische\\_Zusammenarbeit\\_der\\_ND\\_Vortrag%20\\_042008.pdf](http://www.hans-georgwieck.com/data/Eu%E4ische_Zusammenarbeit_der_ND_Vortrag%20_042008.pdf). Consulta efectuada 20 enero 2013.

463 Julia Pulido, “El papel de la inteligencia en la PESD”, *Cuadernos de Estrategia*, N° 130. Ministerio de Defensa de España, 2005, p. 282.

464 Julia Pulido, “Inteligencia: la 'savia' de la Unión Europea”, *Inteligencia y Seguridad: Revista de Análisis y Prospectiva* N° 7 (Diciembre 2009– Mayo 2010). Cátedra Servicios de Inteligencia y Sistemas democráticos (Universidad Rey Juan Carlos) Instituto Juan Velázquez de Velasco de Investigación para la Seguridad y Defensa (Universidad Carlos III de Madrid), España, pp. 92-93.

465 El organigrama donde es posible ver esquemáticamente el lugar donde se ubica actualmente este organismo, está disponible en [http://eeas.europa.eu/background/docs/organisation\\_en.pdf](http://eeas.europa.eu/background/docs/organisation_en.pdf).

466 Chris Jones, “Secrecy reigns at the EU’s Intelligence Analysis Centre”, *Statewatch*. Disponible en <http://www.statewatch.org/analyses/no-223-eu-intcen.pdf>. También fue consultado Iikka Sami, *Parlamento Europeo*. Disponible en [http://www.europarl.europa.eu/meetdocs/2009\\_2014/documents/sede/dv/sede041011cvsalmi/sede041011cvsalmi\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede041011cvsalmi/sede041011cvsalmi_en.pdf).

467 Julia Pulido, “Inteligencia: la 'savia' de la Unión Europea”, *op. cit.*, p. 87-107.

468 Tim Schumacher, *op. cit.*

469 Francisco Veiga, “ECHELON, en control directo”, en *El desequilibrio como orden: Una historia de la posguerra fría 1990 – 2008* (España: Alianza Editorial, 2009).

470 Antonio Díaz Fernández, *op. cit.*, p. 14.

471 Antonio Díaz, Miguel Revenga, Oscar Jaime y Rafael Martínez, Hacia una política europea en inteligencia, *Revista Política Exterior* (España), Vol XIX, N° 106 (Agosto 2005), p. 31.

## Russell G. Swenson y Carolina Sancho Hirane

472 Antonio Díaz Fernández, *op. cit.*, p. 32.

473 Antonio Díaz Fernández, “Evolución de la cooperación europea en inteligencia”, *Varia Historia* (Belo Horizonte), 28, N° 47 (2012), pp. 184-185.

474 Antonio Díaz, Miguel Revenga, Oscar Jaime, y Rafael Martínez, *op. cit.*, p. 26.

475 Ejemplos al respecto pueden encontrarse en Antonio Díaz, (coord.), Miguel Revenga, y Oscar Jaime, *Cooperación en Inteligencia* (España: Thomson Reuters / IUGM, 2009) y en Anselmo del Moral Torres, *Cooperación Policial en la Unión Europea* (España: Dirección General de la Policía, Ministerio del Interior / Dykinson, 2011).

476 José Manuel Ugarte, “Aportes y propuestas para la cooperación de Inteligencia”, *op. cit.*, p. 194.

477 Tratado Constitutivo de UNASUR. Disponible en [http://www.unasursg.org/index.php?option=com\\_content&view=article&id=290&Itemid=339](http://www.unasursg.org/index.php?option=com_content&view=article&id=290&Itemid=339). Consultado el 1 febrero 2013.

478 Tratado Constitutivo de UNASUR.

479 Un mayor desarrollo se encuentra en el proyecto de investigación extramuro n° ext/12/2012, autora Carolina Sancho Hirane, “Cooperación en Inteligencia y Unasur: Posibilidades y Limitaciones”, ANEPE, Chile. 2013.

480 “Valores, principios y seguridad en la comunidad Iberoamericana de Naciones”, *Cuaderno de Estrategia* N° 126, IEEE / Ministerio de Defensa España. Disponible en <http://www.ieee.es/Galerias/fichero/cuadernos/CE-126.pdf>. Consultado 10 enero 2013.

481 Al respecto se recomienda revisar las páginas institucionales de cada uno de estos dos organismos, las cuales han sido consultadas en 15 noviembre 2012. La página WEB de CLACIP está disponible en <http://www.clacip.org/>. La página WEB de INTERPOL está disponible en <http://www.interpol.int/es/>.

482 National Research Council of the National Academies, *Maritime Security Partnerships* (Washington, DC: The National Academies Press, 2008), p. 217.

483 Extraído de la página Web de GAFISUD. Disponible en <http://www.fatf-gafi.org/pages/financialactiontaskforceofsouthamericaagainstmoneylaunderinggafisud.html>. Consultado 15 noviembre 2012.

## Gestión de Inteligencia en las Américas

484 Extraído de la página Web de GAFISUD.

485 Extraído de la página Web de Aduanas de Chile. Disponible en [http://www.aduana.cl/prontus\\_aduanas/site/artic/20070227/pags/20070227233346.html](http://www.aduana.cl/prontus_aduanas/site/artic/20070227/pags/20070227233346.html). Consultado 1 marzo 2013.

486 José Manuel Ugarte, “Aportes y propuestas para la cooperación de inteligencia”, *op. cit.*, p. 175.

487 *Ibid.*, p. 175.

488 *Ibid.*, p. 176.

489 *Ibid.*, p. 182.

490 *Ibid.*, p. 183.

491 *Ibid.*, p. 194.

492 Véase la página web en <http://www.unasursg.org/inicio/documentos/consejos-sectoriales/consejo-suramericano-en-materia-de-seguridad-ciudadana-justicia-y-coordinacion-de-acciones-contr-la-delincuencia-organizada-trasnacional>.

493 Richard A. Clarke y Robert K. Knake, *Guerra en la red* (España: Ariel, 2011).

494 José Manuel Ugarte, “Aportes y propuestas para la cooperación de inteligencia”, *op. cit.*, pp. 157-158.

495 Al respecto se recomienda Javier Jordán, “Introducción al análisis de inteligencia”, Grupo de Estudios en Seguridad Internacional (GESI), España (2011). Disponible en <http://seguridadinternacional.es/gesi/es/contenido/introducci%C3%B3n-al-an%C3%A1lisis-de-inteligencia>; y Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999). Disponible en <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/>. Búsqueda de ambos efectuada 10 octubre 2012.

496 José Manuel Ugarte, “Aportes y propuestas para la cooperación de inteligencia”, *op. cit.*, p. 160.

497 Mónica Serrano, “Crimen transnacional organizado y seguridad internacional: cambio y continuidad”, en Mats Berdal y Mónica Serrano, (comps.), *Crimen trans-*

*nacional organizado y seguridad internacional* (México: Fondo de Cultura Económica, 2005), p. 47.

498 Mónica Den Boer, "Cooperación para la aplicación de la ley y crimen transnacional organizado en Europa", en Mats Berdal y Mónica Serrano, *op. cit.*, p. 174.

499 Asimismo, una institucionalizada cooperación en inteligencia como se plantea en este trabajo, también enfrenta desafíos. Al respecto resulta de interés la experiencia de EE.UU. en esta materia. Sobre este tema se recomienda, Bridget Rose Nolan, "Information Sharing and Collaboration in The United States Intelligence Community: An Ethnographic Study of the National Counterterrorism Center", PhD dissertation, University of Pennsylvania, 2013.

500 Ejemplo de ello ha ocurrido recientemente en el caso de Bolivia, cuando el máximo jefe antidrogas fue detenido por participar en el negocio de este ilícito. Su arresto ha afectado la cooperación en inteligencia, particularmente con Chile, porque el servicio de inteligencia que encabezaba queda desprestigiado y muy particularmente porque su detención fue en territorio chileno en una operación conjunta con la DEA (Drug Enforcement Administration) de EE.UU. Al respecto se recomienda "Ex Zar antidrogas boliviano se declara culpable en EE.UU. de tráfico de drogas a través de Chile", *La Tercera*, 24 junio 2011. Disponible en <http://diario.latercera.com/2011/06/24/01/contenido/pais/31-73881-9-ex-zar-antidrogas-boliviano-se-declara-culpable-en-eeuu-de-trafico-a-traves-de.shtml>. Consulta efectuada 5 febrero 2013.

501 José Manuel Ugarte, "Aportes y propuestas para la cooperación de inteligencia", *op. cit.*, p. 161.

502 Juez Barrington Parker, refiriéndose a Richard Helms, ex Director de Inteligencia Central, acusado de mentir a una comisión del congreso durante su mandato, para proteger los secretos de la CIA. Citado por Paul Gordon Lauren, "Ethics and Intelligence", en *Intelligence, Policy and Process*, ed. por Alfred C. Maurer, Marion D. Tunstall y James M. Keagle (Boulder, Colorado: Westview Press, 1985), p. 72.

503 Sobre las diversidades entre la actividad de inteligencia en un Estado democrático y en un Estado totalitario, véase José Manuel Ugarte, "Sistemas de Inteligencia y Democracia", en Bernardo Arévalo de León (comp.), *Función Militar y Control Democrático* (Ciudad de Guatemala: UNOPS, El Amanuense, 2001), pp. 182-185.

504 José Manuel Ugarte, "Aportes y propuestas para la cooperación de inteligencia", *op. cit.*, pp. 177-236.

## Gestión de Inteligencia en las Américas

505 Adoptada en San José, Costa Rica el 22 noviembre 1969. Véase [http://www.oas.org/dil/esp/tratados\\_B-32\\_Convencion\\_Americana\\_sobre\\_Derechos\\_Humanos.htm](http://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm). Consultado 23 enero 2013.

506 Sobre este aspecto, Peter Gill señaló que “un mandato legal restricto [para los organismos de inteligencia de seguridad] no es una condición suficiente para el control de estos organismos...pero es una condición necesaria”. Véase *Policing Politics: Security Intelligence and the Liberal Democratic State* (London: Frank Cass, 1994), p. 127.

507 José Manuel Ugarte, *El control público de la actividad de inteligencia en América Latina* (Buenos Aires: Editorial Ciccus, 2012), p. 88.

508 Título V, *De los procedimientos especiales de obtención de información*, artículos 23 a 32.

509 Sección 21, subsección 3 de la *Ley del Servicio Canadiense de Inteligencia de Seguridad*.

510 En Chile, la denominación de fuerzas del orden y la seguridad corresponde a las instituciones de naturaleza policial, en el caso Carabineros de Chile y la Policía de Investigaciones.

511 Bien que establece que “en todo caso, la interceptación de comunicaciones estará sujeta a los procedimientos establecidos por el artículo 15 de la Constitución y el Código de Procedimientos Penal” (artículo 42, tercer párrafo).

512 Ello, sin perjuicio de establecer la existencia de control judicial de la seguridad democrática en los términos establecidos por la legislación del país, artículo 6, numeral 4 y artículo 13 de la referida ley 750, del 2010. Disponible en <http://legislacion.asamblea.gob.ni/Normaweb.nsf/b92aeea87dac762406257265005d21f718c11614758755b3a062578240073f60a?OpenDocument>. Consultado 12 octubre 2012.

513 Decreto Legislativo N° 18-2008. Sin perjuicio de establecer el control judicial sobre las actividades que por mandato constitucional y legal requieran dicho control, remite a las leyes sobre la materia (artículo 34).

514 Disponible en <https://www.avid.nl/english/avid/the-intelligence-and/#Documents>. Consultado 10 octubre 2012.

515 Ley N° 9883, artículos 1 apartado 2 y 4. Véase de José Manuel Ugarte, “El ámbito normativo de la inteligencia interior en América Latina”, *Revista Vária História*, 28, N° 47 (Belo Horizonte), junio 2012. Disponible en <http://www.scielo.br>. Consultado 15 diciembre 2012.

516 Hemos descrito el fenómeno representado por el surgimiento en América Latina de la *inteligencia criminal*, en nuestros artículos “La actividad de inteligencia en América Latina y el surgimiento de la inteligencia criminal”, ponencia presentada en Latin American Studies Association, Montreal, 2007, hoy disponible, entre otras localizaciones, en [www.resdal.org](http://www.resdal.org) (consultado 10 octubre 2012) y en “La evolución de la actividad de inteligencia y de la inteligencia criminal en América Latina: Actualidad, dificultades, perspectivas y propuestas”, Rio de Janeiro, 2009, hoy incluida en el libro de José Manuel Ugarte, *Actividad de Inteligencia y Democracia en América Latina* (Saarbrücken, Alemania: Editorial Académica Española, 2011).

517 Representantes del órgano de inteligencia de la Policía Federal y del ámbito operacional de la Policía Caminera Federal, dos representantes del Ministerio de Hacienda -de las áreas de control de actividades financieras y de investigación tributaria- dos representantes del Ministerio de Defensa, un representante del Gabinete de Seguridad Institucional de la Presidencia de la República, un representante de Defensa Civil del Ministerio de Integración Nacional, y un representante de la ABIN.

518 Aunque ello procuró ser posteriormente atenuado por la creación del Consejo Nacional de Jefes de Organismos de Inteligencia de Seguridad Pública-CONCOI- previsto en la Resolución No. 1/2009 de la SENASP-MJ- resulta evidente el carácter de paliativo que tuvo tal creación, ante la menor importancia de este último órgano, respecto del primero.

519 No creo que pueda considerarse estrictamente al Centro Estratégico de Análisis del Delito de Chile como un organismo de inteligencia criminal, dado que su rol se limita a efectuar análisis del delito sobre la información que le remiten las instituciones que en Chile cumplen los roles fundamentales en el sistema penal; y, por otra parte, que el análisis es realizado por analistas que representan a tales instituciones. Es decir, no tiene capacidades propias para cumplir las funciones del ciclo de la inteligencia.

520 En el interesante blog *Inteligencia Policial*, en el artículo “Inteligencia de Seguridad Pública y DNISP- Aspectos Iniciales”, colocado por el delegado de Policía Civil y profesor Emerson Wendt, se afirma que “la DNISP quedó literalmente con un contenido ‘clásico’ de inteligencia de Estado y pocos conceptos, directivas, y acciones específicas de inteligencia de seguridad pública o, hasta más

## Gestión de Inteligencia en las Américas

específicamente, de inteligencia policiales, fueron insertados”. Disponible en <http://www.inteligenciapolicial.com.br/2010/03/inteligencia-de-seguranca-publica-e.html>. Consultado 19 noviembre 2012.

521 Michael D. Bayer, *The Blue Planet: Informal International Police Networks and National Intelligence* (Washington, DC: National Defense Intelligence College, 2010).

522 Remitimos sobre este aspecto a, exposición de José Manuel Ugarte, “Actividad de inteligencia en el hemisferio y el espíritu de las Conferencias de Ministros de las Américas: Cooperación subregional y regional y fortalecimiento institucional en la materia”, Conferencia Subregional 2011, Center for Hemispheric Defense Studies y Ministerio de Defensa Nacional de Chile, Santiago de Chile, 19-22 julio 2011.

523 Véase de José Manuel Ugarte, “La inteligencia criminal en la seguridad pública argentina”, en Enrique del Percio (coord.), *Prejuicio, crimen y castigo* (Buenos Aires: Editorial Sudamericana, 2010).

524 Jerry H. Ratcliffe, *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders*, Second Edition (Washington, DC: COPS-Police Foundation, 2007), p. 8.

525 Sobre el Modelo Nacional de Inteligencia inglés, remitimos a, de José Manuel Ugarte, “La inteligencia Criminal en el Reino Unido y Canadá”, 2ª Parte, *Revista de Policía y Criminalística*, N° 18 (marzo de 2007), Editorial Policial, Buenos Aires.

526 Una breve referencia sobre el Modelo Europeo de Inteligencia, se encuentra en, de Hugo Brady, *Europol and the European Criminal Intelligence Model: A Non-state Response to Organised Crime* (España: Real Instituto Elcano, 2007), disponible en [http://www.realinstitutoelcano.org/wps/portal/riecano\\_eng/Print?WCM\\_GLOBAL\\_CONTEXT=/wps/wcm/connect/elcano/Elcano\\_in/Zonas\\_in/ARI126-2007](http://www.realinstitutoelcano.org/wps/portal/riecano_eng/Print?WCM_GLOBAL_CONTEXT=/wps/wcm/connect/elcano/Elcano_in/Zonas_in/ARI126-2007). Consultado 4 enero 2013. Cabe destacar también en materia de intercambio de información policial, en la Unión Europea, del Consejo de Europa, los Programas de La Haya (2005/C 53/01) y de Estocolmo (2010/C 115/01).

527 Decreto-Ley 2859 de 1979, artículo 1°, texto según Ley N° 20426, disponible en [www.leychile.cl](http://www.leychile.cl). Consultado 25 diciembre 2012.

528 Información contenida en la página de Gendarmería de Chile, [www.gendarmeria.gob.cl](http://www.gendarmeria.gob.cl). Consultado 26 diciembre 2012.



529 Inició sus actividades el 19 de abril de 2011. Amplios detalles sobre el CEAD pueden obtenerse en <http://www.seguridadpublica.gov.cl>. Consultado 4 enero 2013.

530 En América Latina, la doctrina de inteligencia suele distinguir entre “organismo de inteligencia”, organismo técnico especializado en inteligencia, con capacidades para cumplir todas las funciones del ciclo de inteligencia, y “órgano de inteligencia”, capacitado para cumplir sólo parte de tales funciones. El órgano chileno referido, el Centro Estratégico de Análisis del Delito de Chile, constituiría estrictamente un órgano de análisis.

531 Adherimos a la concepción (fundamentalmente inglesa y australiana) que considera al análisis del delito, parte de la inteligencia criminal.

532 En efecto; en Estados Unidos, la Orden Ejecutiva N° 12333, de 1981, no menciona expresamente al Federal Bureau of Prisons, dependiente del Departamento de Justicia, entre los elementos de la Comunidad de Inteligencia. Tampoco en el Reino Unido, la Ley de los Servicios de Inteligencia de 1994 hace mención de la inteligencia penitenciaria, como en Italia la Ley del 2007 no los incluye dentro del Sistema de Información para la Seguridad de la República (artículo 2), como tampoco lo hace la Ley Orgánica de los Servicios de Inteligencia y Seguridad de 1998 del Reino de Bélgica ni ninguna ley orgánica de inteligencia, hasta donde llega nuestra memoria.

533 Véase de José Manuel Ugarte, “La actividad de inteligencia en América Latina: De las reformas formales a las reformas legales”, ponencia presentada en Latin American Studies Association, San Francisco, disponible, entre otras localizaciones, en [www.aainteligencia.cl](http://www.aainteligencia.cl). Consultado 20 diciembre 2012.

534 Elizabeth Sepper, “Democracy, Human rights, and Intelligence Sharing”, *Texas International Law Journal*, no. 46 (otoño 2010), p. 150.

535 El artículo 1 del Código Penal argentino establece que “Este código se aplicará: 1) Por delitos cometidos o cuyos efectos deban producirse en el territorio de la Nación Argentina, o en los lugares sometidos a su jurisdicción; 2) Por delitos cometidos en el extranjero por agentes o empleados de autoridades argentinas en desempeño de su cargo. Normas similares existen en otros países.

536 Remitimos para una visión comparativa a, de José Manuel Ugarte, *El Control Público de la Actividad de Inteligencia en América Latina* (Buenos Aires: Editorial CICCUS, 2012).

## Gestión de Inteligencia en las Américas

537 Por lo general, los organismos de inteligencia militares o dependientes de los Ministerios de Defensa.

538 Los órganos de control externo de la actividad de inteligencia en Latinoamérica carecen de facultades para acceder a materias clasificadas, o deben recurrir para ello a algún tipo de intermediación; así como, en su mayoría, de personal y medios materiales adecuados para ejercer sus responsabilidades.

539 Peter Gill, “Democratic and Parliamentary Accountability of Intelligence Services After 9/11”, en Hans Born y Marina Caparini (eds.), *Democratic Control of Intelligence Services* (Ashgate, UK: Aldershot, 2007), p. 213.

540 Jeffrey T. Richelson y Desmond Ball, *The Ties That Bind: Intelligence Cooperation between the UKUSA Countries* (Sydney, Australia: Allen & Unwin, 1985). Como formal y permanente, esta cooperación comprendió a Estados Unidos de América, Reino Unido, Australia, Canadá y Nueva Zelanda en materia de inteligencia de señales (SIGINT), instrumentada en el Acuerdo UK/USA o Tratado Secreto, con división de áreas de responsabilidad, configurando posteriormente el sistema *ECHELON*. El acuerdo sumó de manera parcial e incompleta a otros países.

541 Martin S. Alexander, “Introduction: Knowing Your Friends, Assessing Your Allies—Perspectives on Intra-Alliance Intelligence”, en Martin S. Alexander, (ed.), *Knowing Your Friends* (London: Frank Cass, 1998), pp. 1-17.

542 Michael Herman, *Intelligence Power in Peace and War*, quinta reimpresión (Cambridge, UK: Royal Institute of International Affairs, Cambridge, 2003), p. 200.

543 Michael Herman, *op. cit.* pp. 203-204.

544 Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information* (Cambridge, UK: Cambridge University Press, 2001), p. 219.

545 Shlomo Schapiro, *The Communication of Mutual Security: Frameworks for European-Mediterranean Intelligence Sharing* (Israel: Department of Political Studies, Bar-Ilan University, 2001), pp. 4-5. Disponible en <http://www.nato.int/acad/fellow/99-01/shapiro.pdf>. Consultado 5 enero 2013.

546 Además de lo que puede extraerse sobre ello del trabajo de Priscila Brandão en comentario, véase de José Manuel Ugarte, *Un nuevo examen de las estructuras de inteligencia en América Latina, Mirador de Seguridad* (Managua, Nicaragua: Instituto de Estudios Estratégicos y Políticas Públicas, 2006), disponible en <http://www.fasoc.cl/files/observatorio/OBS44172ac9ed839.pdf>. Consultado 20 diciembre

2012; “La actividad de inteligencia en América Latina y el surgimiento de la inteligencia criminal”, ponencia presentada en Latin American Studies Association, Montreal, 2007, disponible en [www.resdal.org/lasa/lasa07-ugarte.pdf](http://www.resdal.org/lasa/lasa07-ugarte.pdf). Consultado 20 diciembre 2012; y “La evolución de la actividad de inteligencia y de la inteligencia criminal en América Latina”, ponencia presentada en Latin American Studies Association, Rio de Janeiro, 2009, incluido en el libro, de José Manuel Ugarte, *Actividad de inteligencia y democracia en América Latina (Saarbrücken, Alemania: 2011)*.

547 Hemos descripto ese interesante fenómeno en el trabajo “Actividad de inteligencia en el hemisferio y el espíritu de las Conferencias de Ministros de las Américas: Cooperación subregional y regional y fortalecimiento institucional en la materia”, ponencia presentada en la Conferencia Subregional del Cono Sur, Santiago de Chile, julio de 2011.

548 John Casey, *Policing the World: The Practice of International and Transnational Policing* (Durham, North Carolina: Carolina Academic Press, 2010), p. 155.

549 Governabilidade implica a capacidade de um determinado sistema sócio-político para governar a si mesmo, no contexto de outros sistemas mais amplos.

550 Para uma discussão sobre a importância da definição conceitual na área de inteligência ver Rodrigo Iennaco, *Inteligência Criminal e Denúncia Anônima* (Belo Horizonte: Arraes Editores, 2011).

551 Domício Proença em comunicação pessoal com a autora.

552 *Idem*.

553 Eduardo Estevez, “Estructuras y su aplicación en policías en proceso de reforma,” em *Inteligencia policial—compilación de textos* (Guatemala: Instituto de Enseñanza para el Desarrollo Sostenible, 2000), p. 38.

554 Corporativismo aqui deve ser compreendido pelo seu aspecto negativo, no qual colegas de uma determinada instituição esforçam-se por escamotear seus erros em relação às instituições similares, atuando como um corpo fechado, dotado de dinâmica própria, e que prima pela rivalidade pura e simples, face às diferenças histórico-institucionais, ao invés de atuar em cooperação.

555 Luiz Eduardo Soares (Edição 1 - 2006), *Segurança tem saída* (Rio de Janeiro: Sextante, 2011), p. 33.

## Gestão de Inteligência em las Américas

556 *Ibid.*, pp. 36, 63.

557 *Ibid.*, p. 117.

558 *Ibid.*, p. 118.

559 [http://www.dhnet.org.br/3exec/novapolicial/plano\\_segpub.htm](http://www.dhnet.org.br/3exec/novapolicial/plano_segpub.htm).

560 Para esta discussão, ver: Priscila Brandão, *Serviços Secretos e Democracia no Cone Sul* (Niterói: Impetus, 2010).

561 Decreto 3695, 21 dezembro 2000.

562 No Brasil, as “polícias militares” são parte das forças armadas apenas enquanto força de reserva (artigo 144 da Constituição). São instituições subordinadas dos 26 estados e do Distrito Federal, e têm como função a manutenção da ordem pública, enquanto a Polícia Civil é responsável por realizar investigações criminais.

563 Relatório Ministério da Justiça – I Seminário Nacional sobre Atividade de Inteligência de Segurança Pública, Blue Tree Park, Brasília-DF, 5, 6 e 7 de dezembro de 2001.

564 *Ibid.*

565 *Ibid.*

566 Programa – II Seminário Nacional sobre a Atividade de Inteligência de Segurança Pública, 27 a 29 de novembro de 2002 em Brasília-DF.

567 Decreto Nº 4685, 29 abril 2003.

568 Rômulo Gomes Fonini, *Compartilhamento de informações entre os órgãos de inteligência de segurança pública no país*, monografia apresentada à Fundação Escola Superior do Ministério Público/Newton Paiva (Belo Horizonte, 2010).

569 Vários depoentes afirmaram terem se assustado com a diferença, em termos de atenção, concedida aos alunos e ao curso propriamente dito, principalmente na cerimônia de encerramento.

570 Portaria 22, 22 julho 2009, publicada no *Diário Oficial*.

571 Entrevista realizada sob condição de sigilo, em Brasília, 26 julho 2006.

572 Resolução Nº 1, CESISP, 15 julho 2009.

573 Entrevista realizada com Anderson Aparecido dos Anjos, aluno da especialização, atual Subsecretário Estadual de Inteligência, do governo do Mato Grosso. Entrevista realizada em Cuiabá, em fevereiro de 2009.

574 Doutrina Nacional de Segurança Pública. Versão impressa, desclassificada, de distribuição restrita, divulgada entre os presentes durante encontro realizado por ocasião dos preparativos para o XV Jogos Pan-Americanos, em julho de 2007.

575 Robert Blitzer, “Attorney General Guideline Changes Impacting FBI Intelligence Collection Operations”, The George Washington University Homeland Security Policy Institute, 15 junho 2011. Disponível em <http://securitydebrief.com/2011/06/15/attorney-general-guideline-changes-impacting-fbi-intelligence-collection-operations/>. Acessado 27 dezembro 2011.

576 Decreto 7364, 23 novembro 2010. Disponível em <http://www.jusbrasil.com.br/legislacao/1025747/decreto-7364-10>. Acessado 19 dezembro 2011.

577 Para uma análise sobre o orçamento militar ver: Patrícia de Oliveira Mattos, “Orçamento e Defesa Nacional: uma análise da participação do setor de defesa no orçamento federal de 2000 a 2009”, em: III *Seminário de Estudos: Poder Aeroespacial e Estudos de Defesa - Anais*, 2010. v. II. pp. 439-459. Disponível em: [http://www.unifa.aer.mil.br/seminario3\\_pgrad/trabalhos/patricia-de-oliveira-matos.pdf](http://www.unifa.aer.mil.br/seminario3_pgrad/trabalhos/patricia-de-oliveira-matos.pdf). Acessado 3 janeiro 2012.

578 Leandro Fortes, “Nós, os inimigos”, Seção Seu País *Revista Carta Capital*, edição 668, 14 outubro 2011. Disponível em <http://www.cartacapital.com.br/political/nos-os-inimigos-2/>. Acessado 3 janeiro 2012. Destaque da autora.

579 Domicio Proença Júnior e Eugênio Diniz, *Política de Defesa no Brasil: uma análise crítica* (Rio de Janeiro: Edições Humanidades, 1998).

580 *Ibid.*, p. 42.

581 Neste debate agradeço a interlocução estabelecida com Roberto Numeriano, autor de *Serviços Secretos: a sobrevivência dos legados autoritários* (Recife: Editora Universitária, 2010), e Vladimir Brito, autor de *Sistemas de Inteligência no Brasil e nos Estados Unidos*, monografia de especialização (Fundação Escola Superior do Ministério Público de Minas Gerais 2009) e *O papel informacional dos Serviços Secretos*, Dissertação de Mestrado (Pós-Graduação em Ciência da Informação, Universidade Federal de Minas Gerais, 2011).

## Gestão de Inteligência em las Américas

582 Mônica Barroso Ferreira Lacerda, “Processo cíclico e análise de inteligência policial”, artigo recebido pela autora para publicação junto ao livro *Inteligência de segurança pública: Teoria e prática no controle da criminalidade*, em 1 junho 2009.

583 Michael Bayer, *The Blue Planet: Informal International Police Networks and National Intelligence* (Washington, DC: National Defense Intelligence College, 2010), p. 19.

584 *Ibid.*, p. 100.

585 *Ibid.*, pp.17-18.

586 *Ibid.*, pp. 13-15.

587 *Ibid.*, pp. 20-21.

588 *Ibid.*, p. 18.

589 *Ibid.*, p. 37.

590 *Ibid.*, pp. 57, 59.

591 Para informações detalhadas, ver a nova lei que regula o acesso à informação no país: Lei 12527, 18 novembro 2011.

592 Bayer, *op. cit.*, p. 52.

593 *Idem.*

594 *Ibid.*, p. 53.

595 *Ibid.*, pp. 56, 59.

596 A Polícia Federal, por exemplo, possui sua própria doutrina em processo de re-elaboração, sendo que a versão anterior (desatualizada) ainda é inacessível a boa parte dos operadores de inteligência.

597 Relatório Ministério da Justiça – I Seminário Nacional sobre Atividade de Inteligência de Segurança Pública, Blue Tree Park, Brasília-DF, 5, 6 e 7 de dezembro de 2001.

598 Ver por exemplo Edmund F. McGarrell, Joshua D. Freilich, e Steven Chermak, “Intelligence-led Policing as a Framework for Responding to Terrorism”, *Journal of Contemporary Criminal Justice*, 23, Nº 2 (maio 2007), pp. 142-158. Também,

## Russell G. Swenson y Carolina Sancho Hirane

Gregory F. Treverton, e outros, *Moving Toward the Future of Policing* (Washington, DC: RAND Corporation, 2011), pp. 32-39. Disponível em [www.rand.org/content/dam/rand/pubs/.../2011/RAND\\_MG1102.pdf](http://www.rand.org/content/dam/rand/pubs/.../2011/RAND_MG1102.pdf). Acessado 9 janeiro 2012.

599 Para mayor detalle véase Lucia Dammert (coord.), *Reporte del sector seguridad en América Latina y el Caribe* (Santiago, FLACSO Chile, 2007).

600 Organization for Economic Cooperation and Development, *Security System Reform and Governance* (Paris, OECD, 2005), p. 20. Disponible en <http://www.oecd.org/dataoecd/8/39/31785288.pdf>. Consultado 1 Julio 2012.

601 Comisión Interamericana de Derechos Humanos, *Informe sobre seguridad ciudadana y derechos humanos*, 2009, p. 31. Disponible en <http://www.oas.org/es/cidh/docs/pdfs/SEGURIDAD%20CIUDADANA%202009%20ESP.pdf>. Consultado 1 julio 2012.

602 Louis Garzarelli, “Correctional Administrators’ Attitudes: Making a Difference in Correctional Intelligence Gathering and Sharing”, *Corrections Today* (diciembre 2004), p. 119.

603 Edgardo Amaya, *Populismo punitivo: el irracionalismo penal de hoy* [En blog Seguridad y Justicia Penal], 19 septiembre 2006. Disponible en <http://seguridadyjusticia.blogspot.com/2006/09/populismo-punitivo-el-irracionalismo.html>. Consultado 1 julio 2012.

604 Organización de Estados Americanos, *Declaración sobre Seguridad de las Américas* (2003), Sección II (2) del documento, disponible en [www.oas.org/csh/ces/documentos/ce00339s02.doc](http://www.oas.org/csh/ces/documentos/ce00339s02.doc). Consultado 1 julio 2012.

605 Claudia Fuentes y Francisco Rojas, *Promover la seguridad humana, marcos éticos, normativos y educacionales en América Latina y el Caribe* (United Nations Educational, Scientific and Cultural Organization, 2005), p. 52.

606 Garzarelli, *op. cit.*, p.118.

607 Ben Crewe, “The Sociology of Imprisonment”, en Yvonne Jewkes, ed., *Handbook on Prisons* (Portland, Oregon: Willan Publishing, 2007), pp. 123-151.

608 Brian Parry, “Intelligence: The key to Gang Suppression”, *Corrections Today* (abril 2006), p. 42.

609 Crewe, *op. cit.*, p. 125.

## Gestión de Inteligencia en las Américas

610 Dammert, *op. cit.*, p. 123.

611 Ministerio de Seguridad, Presidencia de la Nación, “Misión” (Nº 8). Disponible en <http://www.minseg.gob.ar/mision>. Consultado 1 julio 2012.

612 “El gobierno crea la Secretaría de Inteligencia mediante un decreto”, *Diario en línea Hoy* [Ecuador], 11 junio 2009. Disponible en <http://www.hoy.com.ec/noticias-ecuador/el-gobierno-crea-la-secretaria-de-inteligencia-mediante-un-decreto-352782.html>. Consultado 1 julio 2012.

613 José María Villalta, Proyecto de ley Derogatoria de la Dirección de Inteligencia y Seguridad del Estado y reforma de la Ley General de Policía, Ley Nº 7410, 26 mayo 1994, y sus reformas.

614 “Un proyecto crea inteligencia estratégica para asistir a Evo”, *Radio FM Bolivia*, 15 enero 2010. Disponible en <http://www.fmbolivia.com.bo/noticia21536-un-proyecto-crea-inteligencia-estrategica-para-asistir-a-evo.html>. Consultado 1 julio 2012.

615 “Mujica tiene en su escritorio texto del nuevo proyecto de inteligencia,” *La Red 21* [Montevideo, Uruguay], 27 febrero 2011. Disponible en <http://www.lr21.com.uy/politica/442693-mujica-tiene-en-su-escritorio-texto-del-nuevo-proyecto-de-inteligencia>. Consultado 1 julio 2012.

616 “Crean comisión para redactar ley de inteligencia”, *El País* [Montevideo, Uruguay], 23 noviembre 2011. Disponible en <http://www.elpais.com.uy/111123/ultimo-608285/ultimo-momento/crean-comision-para-redactar-ley-de-inteligencia/>. Consultado 1 julio 2012.

617 Dammert, *op. cit.*, p. 115.

618 Bruce D. Berkowitz y Allan E. Goodman, *Strategic Intelligence for American National Security* (Princeton: Princeton University Press, 1989).

619 Para mayor detalle véase Lucía Dammert y Liza Zúñiga, *La cárcel: problemas y desafíos para las Américas* (Santiago: FLACSO Chile, 2008).

620 Parry, *op. cit.*, pp. 42-45 y Garzarelli, *op. cit.*, pp. 118-121.

621 Elizabeth Sepper, “Democracy, Human Rights and Intelligence Sharing,” 46, no 1, *Texas International Law Journal* (otoño 2010), pp. 151-207. Para una apreciación más amplia del tema, véase *International Intelligence Cooperation and Accountability*, Hans Born, Ian Leigh y Aidan Wills, eds. (London y New York: Routledge, 2011).



622 Gregory F. Treverton, *Reshaping National Intelligence in an Age of Information* (New York: Cambridge University Press, 2001), 137 y Michael Herman, “11 September: Legitimizing Intelligence?” *International Relations* 16, 2 (2002), p. 233.

623 Moisés Naím, *Illicit: How Smugglers, Traffickers and Copycats are Hijacking the Global Economy* (New York: Doubleday, 2005). Al igual que Sepper, Naím señala que el bajo mundo criminal se mueve en espacios internacionales y supranacionales sin gobernanza y opta por la colaboración informal entre países y culturas.

624 H. Bradford Westerfield, “America and the World of Intelligence Liaison,” *Intelligence and National Security* 11, no 3 (julio 1996), pp. 523-524.

625 James Igoe Walsh, *The International Politics of Intelligence Sharing* (New York: Columbia University Press, 2010), p. 4.

626 U.S. Code, Título 50, Capítulo 15, Subcapítulo III, Sección 413b. Disponible en <http://www.gpo.gov/fdsys/pkg/USCODE-2009-title/html/USCODE-2009-title50-chap15-subchapIII-sec413b.htm>.

627 Con algunas excepciones tales como la ley anti-corrupción de EUA – el Acta de Prácticas Corruptas Extranjeras de 1977 que regula los actos de corporaciones estadounidenses en licitaciones internacionales y para asegurar transparencia en prácticas financieras y de contabilidad, y la entrega supranacional pero poco frecuente de criminales notables a la Corte Penal Internacional.

628 Westerfield, *op. cit.*, p. 541.

629 Martin Rudner, “Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism,” *International Journal of Intelligence and CounterIntelligence* 17 (2004), p. 215.

630 Alasdair Roberts, “Entangling Alliances: NATO’s Security of Information Policy and the Entrenchment of State Secrecy,” *Cornell International Law Journal* 36 (2003), pp. 353-354.

631 Sepper, *op. cit.*, nota 99.

632 *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, Official Government Edition (Washington: US Government Printing Office, 2004), pp. 256, 258, 266, 268, 275-276.

633 Ejemplos de convenciones internacionales incluyen la Convención de Ginebra para la protección de no-combatientes y el trato a prisioneros de guerra; diversos

## Gestión de Inteligencia en las Américas

tratados de derechos humanos internacionales; la Convención sobre el Comercio Internacional de Especies Amenazadas de Fauna y Flora Silvestres, y la Convención de Derecho del Mar de las Naciones Unidas.

634 Robert O. Keohane, “The Concept of Accountability in World Politics and the Use of Force”, *Michigan Journal of International Law* 24 (2003), p. 1124. El umbral de rendición de cuentas requiere dos elementos: 1) un mecanismo efectivo para indagar el raciocinio del proceso de toma de decisiones y 2) sanciones costosas para transgresores.

635 *International Journal of Intelligence Ethics*, ISSN 2151-2868, una revista semi-anual que comenzó en la primavera del 2010.

636 Por ejemplo, desde el punto de vista de un observador externo de la NSA, la comunidad UKUSA constituye “un órgano supranacional único, con sus propias leyes, juramentos y lenguaje, ocultos al público.” James Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency—From the Cold War to the Dawn of a New Century* (New York: Doubleday, 2001), pp. 403-404.

637 Ryan Goodman y Derek Jinks, “How to Influence States: Socialization and International Human Rights Law,” University of Chicago and Harvard Law School, Public Law & Legal Theory Research Paper Series, Paper no 95, p. 41, argumenta que la culturización ejercida por algunos Estados que lleva a otros a adoptar prácticas positivas de respeto a los derechos humanos depende en mayor medida de señales de comportamiento positivos y por tanto “no tanto de las propiedades de la regla como las propiedades de la relación del actor con la comunidad.” Artículo disponible en [www.law.uchicago.edu/files/files/g2-Jinks.pdf](http://www.law.uchicago.edu/files/files/g2-Jinks.pdf). Consultado 25 julio 2012.

638 Sepper, *op. cit.*, p. 164.

639 Peter Wright, *Spy Catcher: The Candid Autobiography of a Senior Intelligence Officer* (New York: Viking, 1987). De la portada: “...el gobierno británico se ha esforzado enormemente para evitar la publicación (de este libro)...”

640 Véase Michael D. Bayer, *The Blue Planet: Informal International Police Networks and National Intelligence* (Washington, DC: National Intelligence University, 2010), p. 34 y el capítulo 2 de forma general. Documento disponible en <http://www.ndic.edu/press/18507.htm>.

641 Para leer acerca del ascenso del concepto de seguridad pública, véase la Organización de Estados Americanos en [http://www.oas.org/en/topics/public\\_security.asp](http://www.oas.org/en/topics/public_security.asp). Véase también International Peace Institute (antes International Peace Academy),

*Police Reform Through Community-Based Policing: Philosophy and Guidelines for Implementation* (New York: 2004), disponible en [http://pksoi.army.mil/doctrine\\_concepts/documents/UN/POLICE\\_REFORM.pdf](http://pksoi.army.mil/doctrine_concepts/documents/UN/POLICE_REFORM.pdf), para una reseña de diversas iniciativas. El crecimiento de la actividad policíaca basada en inteligencia es discutida por Jerry H. Ratcliffe, *Intelligence Led Policing* (Portland, Oregon: William Publishing, 2008).

642 Esta es la conclusión que Sepper obtiene de Michael Herman, “Ethics and Intelligence After September 2001,” *Intelligence and National Security* 19, no 2 (verano 2004), véanse de forma especial páginas 346-350.

643 Sepper, *op. cit.*, p. 202.

644 La evidencia más conocida de esta tendencia es la entrega secreta a Estados socios de “combatientes ilegales extraordinarios” seleccionados. Véase Dana Priest, “CIA Holds Terror Suspects in Secret Prisons,” *Washington Post*, 2 noviembre 2005, disponible en <http://www.washingtonpost.com/wp-dyn/content/article/2005/11/01/AR2005110101644.html>. Consultado 3 enero 2013.

645 Sepper, *op. cit.*, p. 203.

646 Sepper, *op. cit.*, pp. 203-204.

647 Bayer, *op. cit.*, capítulo 5.

648 Si bien las cifras comparativas son difíciles de verificar debido a las prioridades internas de diversas agencias, las cifras presupuestales de inteligencia de seguridad nacional contra aquellas de agencias policíacas indica el desequilibrio. El Director de Inteligencia Nacional solicitó un presupuesto de 55 mil millones de dólares para el ejercicio fiscal 2012 para el Programa de Inteligencia Nacional, que no incluye el presupuesto de inteligencia militar, según lo reportado por Steven Aftergood en *Secrecy News*, 15 Febrero 2011, disponible en [http://www.fas.org/blog/secrecy/2011/02/intelbud\\_request.html](http://www.fas.org/blog/secrecy/2011/02/intelbud_request.html). En contraste, el FBI solicitó únicamente 8.3 mil millones para todas sus actividades en el año fiscal 2011. Véase <http://www.fbi.gov/news/testimony/the-fbi-budget-for-fiscal-year-2011>.

649 Mario Villareal Díaz y Juan José Rico Urbiola, “La penalización de las actividades de inteligencia hostil en los órdenes subnacionales de gobierno en México: el caso Nuevo León,” en José Julio Fernández Rodríguez et al., *Cuestiones de Inteligencia en la Sociedad Contemporánea* (Madrid: Ministerio de Defensa, Instituto Español de Estudios Estratégicos, 2001), pp. 175-185. Disponible en [http://www.portacultura.mde.es/Galerias/publicaciones/fichero/Cuestiones\\_inteligencia.pdf](http://www.portacultura.mde.es/Galerias/publicaciones/fichero/Cuestiones_inteligencia.pdf). Consultado 25 julio 2012.

## Gestión de Inteligencia en las Américas

650 Jeanna Cullinan, “Veracruz, Mexico, Fires 980 Police in Corruption Purge,” 20 de octubre de 2011, <http://insightcrime.org/insight-latest-news/item/1729-veracruz-mexico-fires-980-police-in-corruption-purge>. Consultado 3 enero 2013.

651 Spencer Ackerman, “How the Pentagon’s Top Killers Became (Unaccountable) Spies,” *Wired Magazine*, 13 febrero 2012. Disponible en [www.wired.com/danger-room/2012/02/jsoc-ambinder/](http://www.wired.com/danger-room/2012/02/jsoc-ambinder/). Consultado 2 septiembre 2012.

652 Una serie de reportes sobre operaciones militares en el estado mexicano de Veracruz a finales de 2011 fue secundado por un reporte de selección de funcionarios policiales en dicho estado, lo que constituye un ejemplo de la interacción de una institución de seguridad nacional con agencias policíacas. Algunos artículos relevantes son: “México: envían más tropas a Veracruz para contener violencia,” *Noticias 24*, 5 octubre 2011, <http://www.noticias24.com/actualidad/noticia/330158/mexico-envian-mas-tropas-a-veracruz-para-contener-violencia/>; Ronan Graham, “Mexico Installs Federal Forces in Operation to Secure Veracruz,” 6 octubre 2011, <http://www.insightcrime.org/criminal-groups/mexico/gulf-cartel/item/1667-mexico-installs-federal-forces-in-operation-to-secure-veracruz>; “Veracruz suma 980 policías despedidos”, *El Universal*, 10 octubre 2011, <http://www.eluniversal.com.mx/estados/82622.html>. Consultados 3 enero 2013.

653 La co-autora entrevistó a miembros de la policía federal, local y municipal así como a personal del Ejército mexicano, cuyas labores incluyen aspectos internos de seguridad nacional.

654 Es de notar que, en comparación con el ejército, un policía en México no cuenta con apoyo para obtener vivienda, mientras que el ejército tiene prestaciones excelentes como la obtención de créditos de vivienda, de auto, seguros de alta calidad, instalaciones educativas y recreativas, etc.

655 Véase las tablas 8 y 9 de ICESI (2008) ENSI – 5, encuesta de inseguridad en <http://drcureces.files.wordpress.com/2009/12/icesi-5a-encuesta-nacional-sobre-inseguridad.pdf>.

656 La penetración de “el narco” por parte de elementos de inteligencia humana es tan rara que es digno de noticia cuando ocurre. Véase Ginger Thompson, “U.S. Agencies Infiltrating Drug Cartels Across Mexico”, *New York Times*, 24 octubre 2011. Disponible en [http://www.nytimes.com/2011/10/25/world/americas/united-states-infiltrating-criminal-groups-across-mexico.html?pagewanted=1&\\_r=3](http://www.nytimes.com/2011/10/25/world/americas/united-states-infiltrating-criminal-groups-across-mexico.html?pagewanted=1&_r=3). Consultado 3 enero 2013.

657 Ley pública 99-433, “Goldwater-Nichols Department of Defense Reorganization Act of 1986.”

658 Pablo Martínez, “Los nuevos desafíos de la inteligencia en la Republica Argentina,” *Revista de la Escuela Nacional de Inteligencia*, 1, N° 1, Segunda Época (2003), p. 21.

659 Rogers no usa este término, pero es un neologismo que expresa perfectamente bien el entorno de crímenes en el ciberespacio. El término apareció por primera vez en la década de los 70, y sigue siendo usado por estudiosos de ciencias políticas.

660 Rosalba Gamez Alatorre, “Información o formación, en el ciberespacio”, *Contexto Educativo, Revista Digital de Educación y Nuevas Tecnologías*, 4, N° 23 (2002).

661 Ana Rosa Velazco Lozada, “La educación continua como instrumento de desarrollo en el siglo XXI”, *Tendencias, Revista de la Universidad Blas Pascal*, 5, N° 10 (2011), p. 3.

662 Pablo Martinez, “Los nuevos desafíos de la inteligencia en la *Republica Argentina*”, *Revista de la Escuela Nacional de Inteligencia*, 1, N° 1, Segunda Época (2003), p. 21.

663 A modo de ejemplo, la Escuela Nacional de Inteligencia de Argentina (ENI), cuenta con una maestría estructurada dentro del sistema oficial de educación superior con el soporte académico de la Universidad Nacional de La Plata, desde el año 1999. Su oferta es abierta y es requisito de admisión a la carrera que el aspirante posea un título de grado universitario. En el transcurso de su existencia han participado profesionales universitarios de diferentes disciplinas como abogados, cientistas políticos, ingenieros, licenciados en relaciones internacionales, y similares.

664 Andrés Gómez de la Torre Rotta, “Quien vigilará a nuestros vigilantes? (Reinventando a Juvenal ante el foro de Roma en Perú y Sudamérica)”, *Inteligencia y Seguridad: Revista de Análisis y Prospectiva* (España) N° 5 (diciembre 2008-mayo 2009), pp. 49-50.

665 Paul Chaves, “Los espías no bastan: Definiendo las políticas públicas en materia de servicios de inteligencia en Costa Rica”, REDES 2001 (Research and Education in Defense and Security Studies) Center for Hemispheric Defense Studies, Washington, DC, 22-25 May 2001.

## Gestión de Inteligencia en las Américas

666 Miguel Ángel Esteban Navarro, et al., “Gestión del conocimiento y servicios de inteligencia: la dimensión estratégica de la información”, *El profesional de la información*, 12, N° 5 (2003), p. 270.

667 Mensaje del Secretario de Inteligencia de Estado, Acto de clausura del VII Curso Especial de Perfeccionamiento en Inteligencia Estratégica Nacional SIGLO XXI, *Revista de la Escuela Nacional de Inteligencia*, 7, N° 1 (Primer Trimestre 1998), p. 10.

668 Jesús Tramullas Sas, “Tecnologías para la gestión del conocimiento y la generación de inteligencia”, I Seminario sobre Gestión del Conocimiento y Servicios de Inteligencia en el siglo XXI, Universidad Carlos III de Madrid, *Boletín Oficial del Estado*, Instituto Español de Estudios Estratégicos (Madrid, Ministerio de Defensa, abril 2003), p. 67.

669 Tramullas Sas, *op. cit.*, p. 70.

670 Diego Navarro Bonilla, “Introducción”, *Cuadernos de Estrategia* 127, Estudios sobre inteligencia: fundamentos para la seguridad internacional, grupo de trabajo 5/03 (Instituto Español de Estudios Estratégicos, Ministerio de Defensa, España, 2003), p. 20.

671 Especialización: En su transcurso se debe demostrar manejo y aplicación instrumental de conocimientos y la elaboración, presentación y aprobación de un trabajo final o tesina. Maestría o Master: Es un conjunto de actividades organizadas en un área específica del conocimiento destinadas al análisis profundo y sistematizado de la disciplina y a una adecuada formación metodológica para la investigación, demostrada a través del desarrollo de una Tesis. Doctorado: Los Estudios de Doctorado se orientan a formar investigadores para generar aportes significativos al conocimiento en un área específica del saber, desarrollando la capacitación para la realización de un trabajo de investigación original en forma de Tesis.

672 Rocío Santamaría Ambriz, “Los desafíos del postgrado en América Latina”, Colección EDUAL 6, México (1995), p. 21.

673 Walter Barutia Feijoo, “Acreditación universitaria, retos y oportunidades”, *Estudios en Ciencias Administrativas*, Universidad Nacional Mayor San Marcos, Facultad de Ciencias Administrativas Unidad de Postgrado, Peru, 1, N° 1 (2003), pp. 209-210.

674 Se pueden considerar ejemplos de la adopción de la educación superior para la profesionalización del personal de inteligencia, los casos de Argentina (Maestría ENI-Universidad de la Plata), Chile (Magister ACAGUE-Universidad de Chile) o Estados Unidos (Master's Universidad Nacional de Inteligencia/National Intelligence University), aunque cada uno de estos países ha adoptado modalidades diferentes en su aplicación.

675 Carlos Gustavo Arrieta P., et al., "Informe de la Comisión Especial para el DAS", Bogotá, 2006. Entre otros conceptos críticos, se destaca la siguiente observación: "uno de los puntos que recomienda con mayor insistencia la Comisión, es la necesidad de establecer una evaluación externa y periódica de la formación impartida por la Escuela. En efecto, es imprescindible el establecimiento de un riguroso sistema de 'control de calidad', el cual debería ser realizado de manera inmediata y, posteriormente, por lo menos, cada 5 años. En ese mismo sentido, la Comisión recomienda la implementación de programas de actualización permanentes después de que el personal deje la Escuela de formación, de manera que pueda actualizarse periódicamente en las modernas tendencias de la obtención, procesamiento y análisis de la inteligencia y la contrainteligencia."

676 Véase <http://www.esici.edu.col/>.

677 Dispone su catálogo de cursos y publicaciones de su prensa el sitio <http://www.ni-u.edu/index.html>.

678 Relación de cursos impartidos por el CISEN (2000-2008). Véase en [http://www.cisen.gob.mx/site/pdfs/doc\\_desclasificados/21\\_2008\\_CURSOS\\_CAPACITACION\\_2000-2008.pdf](http://www.cisen.gob.mx/site/pdfs/doc_desclasificados/21_2008_CURSOS_CAPACITACION_2000-2008.pdf). Consultado 16 mayo 2012.

679 Guillermo Valdez Castellanos, "Inteligencia para la Seguridad Nacional en el Siglo XXI", *CISEN: 20 años de historia—Testimonios* (México: CISEN, febrero 2009), pp. 14-15. Disponible en [http://www.cisen.gob.mx/site/pdfs/actualidad/La\\_Inteligencia\\_seguridad\\_nacional\\_Valdes.pdf](http://www.cisen.gob.mx/site/pdfs/actualidad/La_Inteligencia_seguridad_nacional_Valdes.pdf). Consultado 16 mayo 2012.

680 Véase <http://www.cisen.gob.mx/site/cisen.htm>.

681 Entrevista al Director del CALEN, General José Burone, 10 enero 2012 en *La Republica Digital*. Véase <http://www.diariolarepublica.net/2012/01/calen-dictara-primer-curso-de-inteligencia-estrategical>. Consultado 10 mayo 2012.

682 *Gaceta Oficial* N° 39.502 de 3 septiembre 2010 de Venezuela, por Decreto N° 7662, se crea la Universidad Militar Bolivariana de Venezuela (UMBV).

## Gestión de Inteligencia en las Américas

683 A través de este criterio de valoración se puede jerarquizar determinada evaluación o actividad asignándole mayor peso.

684 Russell G. Swenson, “¿Para qué sirve una escuela de inteligencia nacional?” Conferencia Magistral, Escuela Nacional de Inteligencia, Perú, 2007.

685 Alberto Bolivar Ocampo, “Prefacio”, en *Profesionalismo de inteligencia en las Américas* (Joint Military Intelligence College, Center for Strategic Intelligence Research, 2004), p. 13. Disponible en [http://www.ni-u.edu/ni\\_press/pdf/Intelligence\\_Professionalism\\_in\\_the\\_Americas.pdf](http://www.ni-u.edu/ni_press/pdf/Intelligence_Professionalism_in_the_Americas.pdf). Consultado 5 junio 2012.

686 Jaime Castillo Arias, “Sistemas de inteligencia: Perspectiva doctrinal para realizar un análisis integral”, *Inteligencia estratégica y prospectiva* (Quito: Facultad Latinoamericana de Ciencias Sociales-FLACSO y Secretaría Nacional de Inteligencia del Ecuador, 2011), p. 98.

687 Álvaro José Venegas González, “Comportamiento profesional en un área de análisis de inteligencia civil estatal colombiana”, *Nova et Vetera* (Colombia) 19, N° 63 (2010), p. 131.

688 William Lynn III, co-creador del concepto de una “Cuarta generación” de guerra, hablando en el Centro para Estudios Estratégicos e Internacionales (CSIS), Fórum de Seguridad Global 2012, 11 abril 2012. Disponible en [http://csis.org/files/attachments/120411\\_FightingACyberWar\\_GSF\\_Transcript.pdf](http://csis.org/files/attachments/120411_FightingACyberWar_GSF_Transcript.pdf). Consultado 11 agosto 2012.

689 Presidente de EE.UU., *Cyberspace Policy Review*, 2009, p. 1. Disponible en [http://www.whitehouse.gov/assets/documents/Cyberspace\\_Policy\\_Review\\_final.pdf](http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf). Consultado 24 julio 2012.

690 Ídem. Esta definición más completa viene del documento del Poder Ejecutivo, *Directiva Presidencial de Seguridad Nacional 54 / Directiva Presidencial de Seguridad Interna 23*. La mayor parte de este documento es clasificado.

691 IT Business Edge, definición del “Espacio cibernético”. Disponible en <http://www.webopedia.com/TERM/C/cyberspace.html>. Consultado 24 julio 2012.

692 Cyberspace.cz, definición “Espacio cibernético”. Disponible en <http://www.cyberspace.cz/>. Consultado 24 julio 2012.

693 Dan Kuehl, “From Cyberspace to Cyberpower: Defining the Problem”, en *Cyberpower and National Security* (Washington, DC: National Defense University



Press, 2009). Disponible en [www.carlisle.army.mil/dime/getDoc.cfm?fileID=181](http://www.carlisle.army.mil/dime/getDoc.cfm?fileID=181), p. 4. Consultado 24 julio 2012.

694 Aunque una discusión completa sobre las implicaciones legales de no incluir “información” como parte de la definición está más allá del ámbito de este ensayo, una complicación para lograr eso aparecería en aquellos países que aplican leyes de fraude a un intruso que obtiene acceso no autorizado en el espacio cibernético (ver descripción de la discusión sobre “intrusión” en el presente ensayo), y luego también aplican leyes de robo para la información que fue accedida.

695 Technopedia, definición de “Ciber ataque”. Disponible en <http://www.technopedia.com/definition/24748/cyberattack>. Consultado 24 julio 2012.

696 Esta definición viene en parte del Jefe del Estado Mayor Conjunto de EE.UU., *JP 1-02 U.S. Department of Defense Dictionary of Military Terms*. Disponible en [http://www.dtic.mil/doctrine/new\\_pubs/jp1\\_02.pdf](http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf). Consultado 24 julio 2012.

697 Esta definición viene de la información presentada en el sitio Web de la Oficina Federal de Investigación de EE.UU. Disponible en <http://www.fbi.gov/about-us/investigate/cyber/computer-intrusions>. Consultado 25 julio 2012.

698 Esta es una definición general parafraseada de la Oficina de Imprenta del Gobierno de EE.UU., Título 18, Código de EE.UU. § 1030, “Fraud and Related Activity in Connection with Computers.” Disponible en <http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-part1-chap47-sec1030.pdf>. Consultado 25 julio 2012.

699 Departamento de Comercio de EE.UU., Publicación Especial del Instituto Nacional de Estándares y Tecnología 800-12, *An Introduction to Computer Security: The NIST Handbook* (Washington, DC: Octubre 1995). Disponible en <http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/index.html>. Consultado 30 Agosto 2012.

700 “Privado” en este uso indica acceso limitado. Por lo tanto, una computadora o red del gobierno que requiere de una clave individual u otra autorización específica es considerada privada, tal y como una computadora y red del sector privado es considerada como privada.

701 David A. Wheeler y Gregory N. Larsen, *Techniques for Cyber Attack Attribution*, IDA Paper P-3792 (Washington, DC: Instituto para el Análisis de Defensa, octubre 2003), p. 1.

## Gestión de Inteligencia en las Américas

- 702 Aquellos curiosos sobre LOIC simplemente pueden buscar “LOIC” en Google.
- 703 Para más detalles sobre botnets y los efectos que pueden causar, véase “Bots & Botnet: An Overview.” Disponible en [http://www.sans.org/reading\\_room/whitepapers/malicious/bots-botnet-overview\\_1299](http://www.sans.org/reading_room/whitepapers/malicious/bots-botnet-overview_1299). Consultado 25 julio 2012.
- 704 U.S.-CERT, “Cyber Threat Source Descriptions”. Disponible en [http://www.us-cert.gov/control\\_systems/csthreats.html#nat](http://www.us-cert.gov/control_systems/csthreats.html#nat). Consultado 25 julio 2012.
- 705 John Brodtkin, “Government-sponsored cyber attacks on the rise, McAfee says”, *Networkworld.com*, 29 Noviembre 2007. Disponible en <http://www.networkworld.com/news/2007/112907-government-cyberattacks.html>. Consultado 25 julio 2012.
- 706 Anna Mulrine, “China is a lead cyberattacker of US military computers, Pentagon reports”, *Christian Science Monitor*, 18 mayo 2012. Disponible en <http://www.csmonitor.com/USA/Military/2012/0518/China-is-a-lead-cyberattacker-of-US-military-computers-Pentagon-reports>. Consultado 26 julio 2012.
- 707 Joel Brenner, *America the Vulnerable* (New York: Penguin Press, 2011), pp. 27-28. Todo el capítulo 2 (pp. 25-43) presenta un resumen útil sobre la actividad criminal.
- 708 Price WaterhouseCoopers Brazil, Ltda, *Cybercrime: Protecting Against the Growing Threat—Global Economic Crime Survey*, noviembre de 2011. Disponible en [http://www.pwc.com/en\\_GX/gx/economic-crime-survey/assets/GECS\\_GLOBAL\\_REPORT.pdf](http://www.pwc.com/en_GX/gx/economic-crime-survey/assets/GECS_GLOBAL_REPORT.pdf). Consultado 26 julio 2012.
- 709 Norton.com. “Cybercrime Report for 2011”, Disponible en <http://now-static.norton.com/now/en/pul/images/Promotions/2012/cybercrime/assets/downloads/en-us/NCR-DataSheet.pdf>. Consultado 4 septiembre 2012.
- 710 Phil Muncaster, “Patriotic hackers face off in South China Sea: Dispute over islands claimed by China and Philippines goes online”, *The Register*. 27 abril 2012. Disponible en [http://www.theregister.co.uk/2012/04/27/philippine\\_china\\_hack\\_stand\\_off/](http://www.theregister.co.uk/2012/04/27/philippine_china_hack_stand_off/). Consultado 11 agosto 2012.
- 711 Kim Zetter, “Report: Hacktivists Out-Stole Cybercriminals in 2011”, *Wired Magazine*, Threat Level blog, 22 marzo 2012. Disponible en <http://www.wired.com/threatlevel/2012/03/hacktivists-beat-cybercriminals/>. Consultado 11 agosto 2012.

## Russell G. Swenson y Carolina Sancho Hirane

712 “Kaspersky Security Bulletin: Malware Evolution 2011”, *Securelist*, 1 marzo 2012. Disponible en [http://www.securelist.com/en/analysis/204792217/Kaspersky\\_Security\\_Bulletin\\_Malware\\_Evolution\\_2011](http://www.securelist.com/en/analysis/204792217/Kaspersky_Security_Bulletin_Malware_Evolution_2011). Consultado 14 agosto 2012.

713 Parmy Olson, *We are Anonymous* (New York: Little, Brown and Company, 2012), pp. 93-94 y 107-112.

714 Asociación de Prensa, “Anonymous claims responsibility for taking down government sites”, *The Guardian*, 8 abril 2012. Disponible en <http://www.guardian.co.uk/technology/2012/apr/08/anonymous-taking-down-government-websites>. Consultado 11 agosto 2012.

715 Olson, *op. cit.*, pp. 280-282.

716 Brian Emery, “LulzSec hits Brazilian websites”, *BBC News*, 22 junio 2011. Disponible en <http://www.bbc.co.uk/news/technology-13878888>. Consultado 11 agosto 2012.

717 THN Security Analyst, “Lulzsec Hack Infraguard Atlanta Members Alliance & Challenge FBI!” *The Hacker News*, 3 junio 2011. Disponible en <http://thehackernews.com/2011/06/lulzsec-hack-infraguard-atlanta-members.html>. Consultado 11 agosto 2012.

718 Ellen Nakashima, “CIA Web Site Hacked; Group LulzSec Takes Credit”, *Washington Post*, 15 junio 2011. Disponible en [http://www.washingtonpost.com/national/national-security/cia-web-site-hacked/2011/06/15/AGGNphWH\\_story.html](http://www.washingtonpost.com/national/national-security/cia-web-site-hacked/2011/06/15/AGGNphWH_story.html). Consultado 11 agosto 2012.

719 John Markoff, “A Most-Wanted Cyberthief Is Caught in His Own Web”, *New York Times*, 16 febrero 1995. Disponible en <http://www.nytimes.com/1995/02/16/us/a-most-wanted-cyberthief-is-caught-in-his-own-web.html>. Consultado 12 agosto 2012.

720 Kevin Mitnik, *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker* (New York: Little Brown and Company, 2011), p. 385.

721 Oficina de Imprenta del Gobierno de EE.UU., 42 USC § 5195c – Critical Infrastructures Protection. Disponible en <http://www.gpo.gov/fdsys/pkg/USCODE-2010-title42/pdf/USCODE-2010-title42-chap68-subchapIV-B-sec5195c.pdf>. Consultado 16 agosto 2012.

722 Véase Google.com. en [http://www.google.com/publicdataexplore?ds=d5bncppjof8f9\\_&met\\_y=it\\_net\\_user\\_p2&idim=country:BRA&dl=en&hl=en&q=brazil+internet+usage#!ctype=l&strail=false&bcs=d&nselm=h&met\\_y=it\\_net\\_user\\_p2&scale\\_](http://www.google.com/publicdataexplore?ds=d5bncppjof8f9_&met_y=it_net_user_p2&idim=country:BRA&dl=en&hl=en&q=brazil+internet+usage#!ctype=l&strail=false&bcs=d&nselm=h&met_y=it_net_user_p2&scale_)

## Gestión de Inteligencia en las Américas

*y=lin&ind\_y=false&rdim=region&idim=region:NAC&idim=country:BRA:USA&ifdim=region&hl=en\_US&dl=en&ind=false*. Consultado 16 agosto 2012.

723 *National Defense Magazine* blog; "For the Satellite Industry, Lines Blur between Military and Commercial Markets", 18 marzo 2011. Disponible en <http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=350>. Consultado 16 agosto 2012.

724 El Acta de Seguridad de Administración de Información Federal de EE.UU. del 2002 asigna responsabilidad y autoridad a agencias federales y otras organizaciones del Poder Ejecutivo para proporcionar ciber seguridad. Para más información sobre esta ley, véase Oficina de Imprenta del Gobierno de EE.UU., 44 U.S.C. § 3541 - Acta de Seguridad de Administración de Información Federal de EE.UU. del 2002. Disponible en <http://www.gpo.gov/fdsys/pkg/USCODE-2011-title44/pdf/USCODE-2011-title44-chap35-subchapIII-sec3541.pdf>. Consultado 6 Septiembre 2012.

725 Toda la información sobre los siete centros proviene de la ilustración "National Cybersecurity Center Policy Capture," presentado en la página web de la Casa Blanca en <http://www.whitehouse.gov/files/documents/cyber/CybersecurityCentersGraphic.pdf>. Consultado 16 agosto 2012.

726 Véase la página de inicio de <http://www.cert.br/en/> para más detalles sobre la misión y subordinación del CERT.br. Consultado 17 agosto 2012.

727 Para un breve resumen del SERPRO, véase [http://www.securities.com/Public/company-profile/BR/SERPRO\\_en\\_1154549.html](http://www.securities.com/Public/company-profile/BR/SERPRO_en_1154549.html). Consultado 17 agosto 2012. El portal de SERPRO ([serpro.gov.br](http://serpro.gov.br)) está en portugués.

728 Luiz Fabricio Thaumaturgo Vergueiro, "Brazilian Security Structure", Federación de Científicos Americanos del Programa de Investigación de Inteligencia. Disponible en <http://www.fas.org/irp/world/brazil/fabrverg.pdf>. Consultado 17 agosto 2012.

729 Unión Europea, *EU/COE Joint Project on Regional Cooperation against Cybercrime: Specialised cybercrime units - Good Practice Study*, Version 9, noviembre de 2011. Disponible en [http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/ Documents/Reports-Presentations/Octopus2011/2467\\_HTCU\\_study\\_V30\\_9Nov11.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/ Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf). Consultado 17 agosto 2012.

730 Isabel Estrada, "Cyberspace Becomes Newest Battlefield for Brazil's Armed Forces", *Diálogo-Américas*, 8 marzo 2011. Disponible en <http://dialogo-americas>.

*com/en\_GB/articles/rmis/features/regional\_news/2011/08/03/aa-brazil-cyber-warfare*. Consultado 17 agosto 2012.

731 Marco Cepik y Priscila Antunes, “The New Brazilian Intelligence Law: An Institutional Assessment”, Centro para los Estudios de Defensa Hemisférica, Investigación y Educación en Estudios de Defensa y Seguridad, mayo 22-25 del 2001, Washington, DC. Disponible en <http://www.fas.org/irp/world/brazil/index.html>. Consultado 5 septiembre 2012.

732 Linha Defensiva, 12 mayo 2012. Disponible en <http://www.linhadefensiva.com/2012/05/brazilian-army-prepares-its-cdciber-the-cyber-defense-center/>. Consultado 17 agosto 2012.

733 Nelson de Sa, “General detalha implantação do Centro de Defesa Cibernética, novo órgão brasileiro”, *Folha de São Paulo*, 5 julio 2012. Disponible en portugués en <http://www1.folha.uol.com.br/tec/1085498-general-detalha-implantacao-do-centro-de-defesa-cibernetica-novo-orgao-brasileiro.shtml>. Consultado 5 septiembre 2012.

734 Emerson Wendt, “Ciberguerra, Inteligencia e segurança virtual: alguns aspectos”, en GSI publicación *Revista Brasileira de Inteligencia*, N.º. 6 (abril 2011), p. 22. Disponible en portugués en [http://www.abingov.br/modules/mastop\\_publish/files/files\\_4e3ae31e2c097.pdf](http://www.abingov.br/modules/mastop_publish/files/files_4e3ae31e2c097.pdf). Consultado 5 septiembre 2012.

735 Para más información, véase <http://www.cert.br/en/>. Consultado 12 septiembre 2012.

736 Cualquiera de las comunidades que pueda ser responsable por el CERT nacional debería tener mayor información sobre la intrusión. No podría proporcionar atribución (quien) inmediatamente, pero podrá distinguir algunos de los detalles sobre donde se originó la intrusión — o por donde pasó. La situación del país A puede ser que hay varios CERTs superpuestos que todos podrían tener conocimiento sobre la intrusión. Si ese fuese el caso, entonces la importancia del intercambio de información es aún mayor: cualquiera de los CERTs pueden tener información importante que los otros no tienen. La superposición de las responsabilidades de CERT es importante para los responsables de inteligencia porque puede incrementar el número de organizaciones con las cuales la información de inteligencia sobre intrusiones necesita ser intercambiada.

737 La obligación de proteger información, al menos para la Comunidad de Inteligencia de EE.UU., se extiende a la protección de la información de personas de EE.UU. que puede ser recopilada casualmente en un esfuerzo para recopilar inteligencia extranjera. La ley de EE.UU. limita estrictamente con quien se inter-

## Gestión de Inteligencia en las Américas

cambia esa información, e inclusive donde se deposita, si es depositada en primer lugar. La discusión detallada de este impedimento está más allá del ámbito de este ensayo, pero para más lectura, véase Oficina de Imprenta del Gobierno de EE.UU (GPO), 50 USC 36, “Foreign Intelligence Surveillance Act of 1978, Amendments Act of 2008”. Disponible en <http://www.gpo.gov/fdsys/pkg/PLAW-110pub1261/html/PLAW-110pub1261.htm>. Consultado 5 septiembre 2012. En los Estados Unidos, los estados de la unión tal vez puedan dirigirse al tema de seguridad cibernética de modo más comprehensiva y agresiva, de acuerdo con la visión de Michael J. Glennon, en su “State-Level Cybersecurity”, *Policy Review* (febrero-marzo 2012).

738 Oficina del Director de Inteligencia Nacional de EE.UU., Directiva de la Comunidad de Inteligencia Numero 208 “Write for Maximum Utility”, 17 diciembre 2008. Disponible en [http://dni.gov/files/documents/ICD/icd\\_208.pdf](http://dni.gov/files/documents/ICD/icd_208.pdf). Consultado 24 agosto 2012.

739 *Idem*.

740 Gobierno de EE.UU., Orden Ejecutiva 12333, párrafo 1.7, “U.S. Government Intelligence Activities”, 4 diciembre 1981. Disponible en <http://www.gpo.gov/fdsys/pkg/FR-2008-08-04/pdf/E8-17940.pdf>. Consultado 28 agosto 2012.

741 Organización de Estados Americanos, “A Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach To Creating a Culture of Cybersecurity”, 2004. Disponible en [http://www.oas.org/juridical/english/cyb\\_pry\\_strategy.pdf](http://www.oas.org/juridical/english/cyb_pry_strategy.pdf). Consultado 29 agosto 2012.

742 Gen. Michael V. Hayden, “The Future of Things Cyber”, *Strategic Studies Quarterly* (primavera 2011), p. 4. Disponible en <http://www.au.af.mil/au/au/ssq/2011/spring/hayden.pdf>. Consultado 5 septiembre 2012.

743 *Idem*.

744 Senadora Dianne Feinstein, “Feinstein Calls on Obama to Protect Computer Networks from Cyber Attacks”, 28 agosto 2012. Disponible en <http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=8c64f8e4-6780-4a4f-88eb-cd26a8839aae>. Consultado 6 septiembre 2012.

745 Chris Strohm, “Obama Weighs Broad Program to Defend Networks from Cyber Attacks”, *Businessweek.com*, 30 agosto 2012. Disponible en <http://www.businessweek.com/news/2012-08-30/obama-weighs-broad-program-to-defend-networks-from-cyber-attacks>. Consultado septiembre 2012.

746 “GCHQ to advise senior business leaders on how to fight cyber attacks”, *Telegraph.co.uk*, 6 septiembre 2012. Disponible en <http://www.telegraph.co.uk/news/uknews/defence/9521715/PLS-PIC-AND-PUB-GCHQ-to-advise-senior-business-leaders-on-how-to-fight-cyber-attacks.html>. Consultado 6 septiembre 2012.

747 Eric Ensign, *The Rum War at Sea, 1920-1933* (Washington, DC: Joint Military Intelligence College, 2001). Disponible en [http://www.ni-u.edu/ni\\_press/pdf/Intelligence\\_Rum\\_War.pdf](http://www.ni-u.edu/ni_press/pdf/Intelligence_Rum_War.pdf). Consultado 11 July 2014.

748 *ISAF Security Force Assistance Guide*, abril 2013. [https://ronna-afghan.harmonieweb.org/CAAT/Shared%20Documents/20130505\\_NIU\\_SFA\\_Guide.pdf](https://ronna-afghan.harmonieweb.org/CAAT/Shared%20Documents/20130505_NIU_SFA_Guide.pdf). Consultado 5 agosto 2013. También ver Liz Panarelli, *The Role of the Ministerial Advisor in Security Sector Reform* (Washington, DC: Instituto de la Paz de EE.UU., abril 2009). Disponible en [http://www.usip.org/files/resources/USIP\\_0409.PDF](http://www.usip.org/files/resources/USIP_0409.PDF). Consultado 7 mayo 2013.

749 Esto también se sostiene por un régimen internacional legal, a lo cual tienen que someterse las fuerzas del extranjero una vez reconocida la soberanía del país anfitrión. El Mayor Andrew R. Atkins proporciona una excelente discusión sobre las complejidades del reconocimiento de soberanía de una nación anfitriona en operaciones militares. Ver “Doctrinally Accounting for Host Nation Sovereignty During U.S. Counterinsurgency Security Operations,” *Military Law Review*, 212 (verano 2012), pp. 70-132.

750 Sarah Meharg y Aleisha Arnush, aunque no se refieran directamente al Poder Inteligente, hacen un argumento similar cuando notan que “de acuerdo con el Manual de Campo (FM) 3-07 del Ejército de Estados Unidos, Stability Operations (2008) [también enfatiza en su Manual de Campo (FM) sucesor 3-22, ver fn. 6 a continuación], SSR es una actividad que puede reforzar intervenciones diplomáticas y de defensa mientras reduce las amenazas de seguridad a largo plazo al construir capacidades para sociedades estables, prósperas y pacíficas”. Ver su *Security Sector Reform: A Case Study Approach to Transition and Capacity Building* (Carlisle, Pennsylvania: Peacekeeping Stability Operations Institute Paper, Security Studies Institute, U.S. Army War College, diciembre 2010, p. 7. Disponible en <http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubid=960>. Consultado 7 octubre 2012.

751 Véase Departamento del Ejército de los Estados Unidos, Manual de Campo (FM) 3-22 Apoyo del Ejército a la Cooperación de Seguridad (Enero 2013), párrafos 4-57 y 4-58: “La tarea de asesoramiento para el nivel gubernamental [SSR] está dirigida a asesorar al personal de alto rango del gobierno extranjero a su nivel

## Gestión de Inteligencia en las Américas

nacional, federal, departamental o ministerial. Las agencias de los Estados Unidos fuera del Departamento de Defensa proporcionan asesoramiento no militar. La tarea de asesoramiento a nivel gubernamental debe incluir un esfuerzo de gobierno entero, integrando agencias de los Estados Unidos como el Departamento de Estado, Tesoro y Justicia...el Departamento de Defensa inició los Asesores del Ministerio de Defensa (conocidos como MoDA), un programa para fomentar relaciones a largo plazo que fortalecen al ministerio de defensa de una nación socia”.

752 Richard L. Armitage y Joseph S. Nye, Jr., *CSIS Commission on Smart Power* (Washington, DC: Center for Strategic and International Studies, 2007). Disponible en [http://csis.org/files/media/csispubs/071106\\_csissmartpowerreport.pdf](http://csis.org/files/media/csispubs/071106_csissmartpowerreport.pdf). Consultado 13 julio 2012. En el presente trabajo adoptamos una perspectiva agnóstica con respecto a la política de Poder Inteligente, y limitamos nuestra atención a los resultados operacionales asociados con reforma del sector de seguridad y el manejo de servicios de inteligencia.

753 Véase Joseph A. Nye para un explicación completa de este concepto de poder blando en seguridad nacional y asuntos externos en *Power: The Means to Success in World Politics* (New York: Public Affairs, 2004), y *Bound to Lead: The Changing Nature of American Power* (New York: Basic Books, 1990).

754 En entrevista hecha por John J. Hamre a los estudiosos de Poder Inteligente, Richard L. Armitage y Joseph Nye, ellos indicaron estar de acuerdo que esta política necesariamente incluye “el ceder de un grado de soberanía nacional”, especialmente “cuando se tratan de instituciones internacionales” (Hamre) pero “toda relación exitosa requiere concesiones mutuas” (Armitage) y “los beneficios son mayores que nuestros costos” (Nye). Véase “Smart Power: John J. Hamre talks with Joseph Nye & Richard Armitage” *The American Interest*, Vol. 3, no. 2 (noviembre/diciembre 2007), pp. 34-41.

755 Sarah Meharg y Aleisha Arnush, *op cit.*, p. iii.

756 David Axe, “The Limits of Smart Power,” *The American Prospect*, 21, no. 10, (diciembre 2010), pp. 23-27; Nicholas J. Armstrong, “Afghanistan 2014-2024: Advising for Sustainability,” *Small Wars Journal* (4 mayo 2012). Disponible en <http://smallwarsjournal.com/author/nicholas-j-armstrong>. Consultado 4 octubre 2012.

757 Manual de Campo del Departamento del Ejército de Estados Unidos 3-22, párrafo 1-61.

758 Liz Panarelli, *op. cit.*, p. 2.



759 *Ibid.*, p. 2.

760 Joseph S. Nye, *The Future of Power* (New York: PublicAffairs, 2011).

761 Suzanne Nossel, "Smart Power: Reclaiming Liberal Internationalism," *Foreign Affairs*, 83, edición 2 (marzo/abril 2004), pp. 131-142.

762 Johanna Mendelson Forman, "Investing in a New Multilateralism – A Smart Power Approach to the United Nations," Centro de Estudios Estratégicos e Internacionales, Iniciativa de Poder Inteligente (enero 2009). Disponible en [http://csis.org/files/media/csis/pubs/090128\\_mendelsonforman\\_un\\_smartpower\\_web.pdf](http://csis.org/files/media/csis/pubs/090128_mendelsonforman_un_smartpower_web.pdf), pp. 1-14. Consultado 5 agosto 2013.

763 Stephen M. Saideman and David P. Auerswald, "Comparing Caveats: Understanding the Sources of National Restrictions upon NATO's Mission in Afghanistan," *International Studies Quarterly*, 56 (marzo 2012), pp. 67-84.

764 William B. Caldwell y Nathan K. Finney, "Building Police Capacity in Afghanistan: The Challenges of a Multilateral Approach," *Prism*, 2, no. 1 (diciembre 2010), pp. 121-129. Disponible en [http://www.ndu.edu/press/lib/images/prism2-1/Prism\\_121-130\\_Caldwell-Finney.pdf](http://www.ndu.edu/press/lib/images/prism2-1/Prism_121-130_Caldwell-Finney.pdf). Consultado 16 octubre 2012.

765 Dennis Steele, "The Closers," *Army Magazine*, 60, no. 4 (Abril 2010), pp. 58-66. La 3ra División de Infantería tuvo la tarea de proporcionar apoyo a los Equipos de Reconstrucción Provincial del Departamento de Estado, mientras realizaba su misión de asesoramiento y asistencia al desarrollo de las fuerzas iraquíes de seguridad; Nicole Ball proporciona una explicación extensa de las intersecciones funcionales en la reforma del sector de seguridad en "Enhancing Security Sector Governance: A Conceptual Framework for UNDP," Consultant Report (octubre 2002), Tabla 1, p. 14. Disponible en [http://www.ssrnetwork.net/uploaded\\_files/3202.pdf](http://www.ssrnetwork.net/uploaded_files/3202.pdf). Consultado 5 septiembre 2012.

766 LTG William B. Caldwell, IV, con Derek S. Reveron, "Surging Security Force Assistance in Afghanistan," *Military Review* (noviembre-diciembre 2011), p. 19.

767 Erving Goffman, *The Presentation of Self in Everyday Life* (New York: Doubleday, 1959). Ver Mark R. Leary y Ashley Batts Watson, "Personality and Persona: Personality Processes in Self-Presentation," *Journal of Personality*, 79, no. 6 (diciembre 2011), pp. 889-916 para una excelente extensión de los conceptos seminales de Goffman.

## Gestión de Inteligencia en las Américas

768 Para más información sobre el programa de Asesores del Ministerio de Defensa ver [http://www.defense.gov/home/features/2011/0211\\_modal/](http://www.defense.gov/home/features/2011/0211_modal/). Para el programa Afghanistan-Pakistan Hands ver <http://www.jcs.mil/page.aspx?id=52>.

769 David A. Klein, "The Strategic Management of Intellectual Capital: An Introduction" en *The Strategic Management of Intellectual Capital*, David A. Klein, (ed.) (Woburn, MA: Butterworth-Heinemann, 1998), pp. 2-3.

770 Mike Pedler, John Burgoyne, y Tom Boydell, *The Learning Company: a Strategy for Sustainable Development*, segunda edición (London: McGraw-Hill, 1997).

771 David A. Klein, *op. cit.*, p. 3.

772 *Ibid.*, p. 4.

773 *Ibid.*, p. 4.

774 Mary M. Crossman, Henry W. Lane y Roderick E. White, "An Organizational Learning Framework: From Intuition to Institution," *Academy of Management Review*, 24, no. 3 (1999), p. 522, citando James G. March, "Exploration and Exploitation in Organizational Learning," *Organization Science*, 2 (1991), pp. 71-87.

775 Ministerio de Defensa del Reino Unido, *Entendimiento y Apoyo de Inteligencia a Operaciones Conjuntas*. tercera ed. Publicación de Doctrina Conjunta 2-00, 30 agosto 2011.

776 *Ibid.*, pp. 1-7.

777 *Ibid.*, pp. 1-8.

778 *Ibid.*, pp. 1-8.

779 *Ibid.*, pp. 1-8.

780 *Ibid.*, pp. 1-8.

781 *Ibid.*, pp. 1-8.

782 *Ibid.*, pp. 1-8.

783 En algunas instancias la relación de asesoramiento es muy cercana y el asesor se considera como un confidente. Cuando esto sucede, la contraparte puede ofrecer un entendimiento detallado al revelar una explicación completa del problema. Aunque es extraordinariamente valioso para un asesor y el liderazgo de la misión de

## Russell G. Swenson y Carolina Sancho Hirane

asesoramiento tener dicha perspectiva directa, no obstante ésta debe ser corroborada porque la contraparte puede, sin perjuicio, ser mal informada o malinterpretar el problema.

784 El Director de Planes Operativos y Desarrollo de Fuerza Conjunta (J-7), *Operaciones Conjuntas, Publicaciones Conjuntas* 3-0 (3 agosto 2011), pp. III-11.

785 Patricia A. Weitsman, *Dangerous Alliances: Proponents of Peace, Weapons of War* (California: Stanford University Press, 2004), p. 35. Ella analiza las variaciones en el nivel de compromiso entre los miembros aliados desde una perspectiva histórica.

786 Thomas Scott Gibson (TRADOC), “CALL publishes Company Intelligence Support Team Handbook,” Centro de Lecciones Aprendidas del Ejército, Fort Leavenworth (25 enero 2009). Disponible en <http://www.army.mil/article/33509/call-publishes-company-intelligence-support-team-handbook/>. Consultado 5 agosto 2013,

787 Jefes de Estado Mayor, AFPAK Hands (APH) Resumen General del Programa (26 de agosto de 2011). Disponible en [http://www.jcs.mil/content/files/2011-09/090811135844\\_AFPAC\\_Hands\\_Program\\_Brief.pdf](http://www.jcs.mil/content/files/2011-09/090811135844_AFPAC_Hands_Program_Brief.pdf). Consultado 27 octubre 2012.

788 Véase [http://www.defense.gov/home/features/2011/0211\\_modal/](http://www.defense.gov/home/features/2011/0211_modal/). Consultado 6 julio 2013.

789 David A. Klein, *op. cit.*, p. 3.

790 Tony Bush, en *Theories of Educational Leadership and Management* (Reino Unido: Sage Publications, Ltd., 2010), extrae de la literatura de dinámicas organizativas para resumir de manera sucinta siete distinciones entre autoridad organizativa e influencia.

791 Véase Michael T. Flynn, James Sisco, y David C. Ellis, “Left of Bang: The Value of Sociocultural Analysis in Today’s Environment,” *Prism*, 3, no. 4, 2 Junio 2013, pp. 13-21. Disponible en: [http://www.ndu.edu/press/lib/pdf/prism3-4/prism12-21\\_flynn-sisco-ellis.pdf](http://www.ndu.edu/press/lib/pdf/prism3-4/prism12-21_flynn-sisco-ellis.pdf); nota: El énfasis de la Agencia Nacional de Inteligencia Geoespacial sobre la geografía humana igualmente con las características físicas e inteligencia de imágenes (Agencia Nacional de Inteligencia Geoespacial, “NGA Strategy 2013-2017,” disponible en: [https://www1.nga.mil/About/NGAStrategy/Documents/19639\\_NGA%20Strat%20Pub\\_Public\\_Web.pdf](https://www1.nga.mil/About/NGAStrategy/Documents/19639_NGA%20Strat%20Pub_Public_Web.pdf), consultado 3 junio 2013. También véase la Oficina del Subsecretario de Inteligencia de Defensa 2010, formalización de Inteligencia en Base a Actividades (ABI) y Análisis de Dominio Humano (HAD).

ÍNDICE (términos en español y portugués)

ABIN (Agência Brasileira de Inteligência) 76, 104, 108, 193, 202, 208, 301-303, 313, 321-323, 337, 339, 341, 351-352, 393, 439

Academia 115, 141, 165, 167, 175, 219, 246, 267, 294, 356, 394-395, 409, 411

Acceso

Abierto 189, 392, 411

a fuentes xxxi, 223-224, 443, 461, 469

a información protegida xxxvi, xl, 36, 299, 356, 427, 429, 433-434, 440-441, 444, 474, 482, 493, 495

a información pública 13, 34-35, 72, 103

a oficiales xxiv, 470

Limitado 472, 484

Actividad

Académica 390-413

Clandestina 224

de asesoramiento 279

de contrainteligencia 16, 21, 148, 239, 373

de cooperación xx, 453-486

Delictiva xxviii, xxx, xxxiii, xxv, 300, 354, 369-370, 375, 429, 431-441

Económica xxxviii, 225, 228, 232, 235, 244-245, 284

Intrusiva 18, 148, 203

Militar xxxiii

Policial xxxiii-xxxiv, 305, 370-371

Sucia 156, 161

Terrorista 154, 205-206, 243

Acuerdos

- Burocráticos xvii
- de cooperación 281-293
- de intercambio de información 309-310, 363, 445-446
- Informales 357
- Internacionales 197, 273, 308, 366
- Políticos 217, 352
- Públicos 130
- Adiestramiento 402, 404, 410
- Aduana 184, 197, 242-244, 284
- Advertencias 232, 235, 243, 247, 430, 439, 441, 472
- Afganistán 121, 383, 453-486
- Agente (véase Inteligencia)
- Agilidad(e) 333-334
- Alemania 127, 141, 164, 280, 304, 401
- Alerta xiv, 31, 86, 206, 209, 232, 235, 238, 252, 265, 278, 288, 307, 375, 437-438, 442
- Aliado 96, 112, 132, 283, 289, 298, 310, 450, 473
- Ambiental 138, 161, 243, 306, 388, 410, 464
- AMERIPOL (Comunidad Americana de Policía) 197, 285
- ANI (Agencia Nacional de Inteligencia, Chile) 20, 78-79, 282, 350, 356, 394
- Anticipar (faceta de inteligencia) xxxv, xxxix, 195, 222, 230, 235-236, 259-260, 287, 349, 439-440, 465, 467, 470-471, 475
- Apreciaciones xvii, xxxix, 29, 49, 212, 216, 242, 246, 361, 404, 426, 465, 467, 477
- Aprendizaje 188, 391, 403, 410, 454, 462-465, 474, 478, 481-482, 490
- Argelia 6, 152-153, 164

## Gestión de Inteligencia en las Américas

### Argentina

Gestión de inteligencia xvii, 213-214, 303, 306, 356

Inteligencia estratégica 128, 134, 193, 282

Ley de inteligencia 20, 26, 76, 117, 147, 299-300, 350

Personal de inteligencia xxviii, 392, 400, 411

Asesoramiento xxv, xxxvi, xli, 52, 190, 384, 409, 414, 453-486

Atentados 145, 158, 213-214, 243, 279, 307, 327

Autonomía (véase Inteligencia)

Autoritarismo 144-145,

BACRIM (Bandas Criminales, Colombia) 206

Bilateral xli, 197-198, 214, 238, 273, 310, 362, 472

Bolivariana (véase Inteligencia)

Bolivia 5, 23, 87, 128, 205-206, 282, 284, 355, 393, 401, 411

### Brasil

Agência Brasileira de Inteligência 104, 134, 202, 208, 313, 321,  
351, 393

Control de inteligencia 3, 93-94, 100, 107, 113, 117

en Haití xvii

Actividad policial xxxii, xxxiv, 206, 305, 319, 331-332, 336

Doctrina de inteligencia 99, 195, 303-304

Gestión de inteligencia xvii, 92, 193

Inteligencia militar xxxvi

Legislación de inteligencia 20, 76-77, 102, 107-108, 147, 300, 335

Ley de acceso a información 3, 103-104, 114

Rendición de cuentas en inteligencia 301

SISBIN (Sistema Brasileira de Inteligência, Brasil) xiv, 20, 301-302,  
317, 321, 323, 393-394

## Russell G. Swenson y Carolina Sancho Hirane

- SISP (Subsistema de Inteligência de Segurança Pública, Brasil) 301-303, 311, 317, 321-323, 325, 341
- SNI (Sistema Nacional de Informação, Brasil) 341, 352, 393
- Sistema de inteligencia brasileña xiv, 91, 282, 301-302, 313, 317-341, 411
- y el ciberespacio 425-451
- Burocracia (véase Inteligencia)
- CAEN (Centro de Altos Estudios Nacionales, Perú) 74, 400, 411
- CALEN (Centro de Altos Estudios Nacionales, Uruguay) 402
- Calidad
- Académica 386, 390-391, 401-423
  - de formación profesional 177, 291, 386-423
  - de información 156, 189, 226, 258
  - de productos de inteligencia 184, 188, 215-216, 218, 251
  - Institucional de inteligencia 151, 386
- Canadá 3, 78, 110-112, 114, 118, 208, 299, 304, 347, 363, 401
- Capacitación xx, 51, 71, 219, 259-260, 281, 283, 287, 357, 385-386, 389-390, 393-410, 416, 489
- Carabineros 165, 283, 306
- Castro, Fidel 126
- Cartel
- Centralizar xxxii, 49-50, 352, 355, 449
- Chile
- Inteligencia militar 136-137, 156, 193
  - Inteligencia penitenciaria 305-306, 314, 343-360
  - Legislación de inteligencia 20, 78-79, 134, 147, 300
  - y comunidad de inteligencia 282, 350, 411
  - y cooperación en inteligencia 196, 283-284

## Gestión de Inteligencia en las Américas

- y rendición de cuentas 118
- China xv, 7, 420, 431
- CIA (Agencia Central de Inteligencia, Estados Unidos) 121, 124-126, 153, 157, 363-364
- Ciberseguridad xl, 381, 436-451, 496
- CICAD (Comisión Interamericana para el Control del Abuso de Drogas) 276, 400-401
- CICTE (Comité Interamericano contra el Terrorismo) 276
- CISEN (Centro de Investigación y Seguridad Nacional, México) 20, 85, 398-399
- Civil (véase Inteligencia)
- CLACIP (Comunidad Latinoamericana y del Caribe de Inteligencia Policial) 197, 283, 285, 292
- Clandestina (véase Actividad)
- Coca 206-207
- Cognitiva ix, 157, 391, 478
- Colaboración (véase Inteligencia)
- Colombia
  - Bacrim 206
  - Chuzadas 134, 202
  - DAS (Departamento Administrativo de Seguridad) 1, 134-136, 202
  - Expectativas 169, 211, 216, 222
  - Inspector general de inteligencia 22, 24
  - Inteligencia económica 182, 194, 221-248
  - Ley de inteligencia 5, 21, 26, 79, 118, 147, 212
  - y personal de inteligencia xxviii, 246-248
- Comercio 221, 228-229, 233, 241-247, 331, 370, 435
- Compartilhamento 320, 334, 340-341



## Russell G. Swenson y Carolina Sancho Hirane

Competencia xxxvii-xxxviii, 26, 33, 47, 49,94, 100-101, 104, 106-110, 138, 153, 223, 227, 263-264, 266, 270, 272, 298, 300-302, 314, 319, 328, 343, 351, 353, 368, 388-389, 450, 461, 464, 469, 488-489

Confiable (véase Inteligencia)

Confianza

de altos oficiales xxii, xxiv, 178, 187-188, 190, 230, 236

Persona de confianza 172, 238

Pública en inteligencia xxxv, 182, 190, 232, 408

y cooperación en inteligencia 276-277, 283, 289-291, 293, 303, 361, 363, 365-366, 383, 445, 454, 474, 476, 482

y servicios de inteligencia xxi, xxxii, 211, 214, 375, 450

Confidencial (información) xxi, xxiv, xxxvi, 35-36, 103, 149, 225, 441, 446, 451

CONPES (Consejo Nacional de Política Económica y Social, Colombia) 245

Consejo

de Defensa Suramericano 217, 272

de Europa 129, 139

de Inteligencia Nacional 41, 43-45, 53, 83, 217

de Ministros 27-28, 38-39, 48-49, 51, 54-55, 60, 70

de Seguridad Pública 21

Gremial Nacional y Cámaras de Comercio 242-243

Nacional de Inteligencia 13

Nacional de Política Económica y Social 245

Superior de Inteligencia 9, 11

Conselho

de Fiscalização do Sistema de Informações da República Portuguesa  
110

## Gestión de Inteligencia en las Américas

- Especial do Secretaria de Inteligência de Segurança Pública 302, 326-327
- Especial do Subsistema de Inteligência de Segurança Pública 322, 324,351
- Nacional de Chefes de Organismos de Inteligência 325-326
- Contrainteligencia 16, 21, 26, 28-31, 40, 42-44, 49-52, 56, 60, 65, 72, 79, 87, 90, 134-135, 148, 152-154, 164, 182, 195, 210, 222-224, 232-234, 237-245, 297, 301, 353, 387-388, 395, 398, 402, 428, 435, 441
- Contraparte 186, 213, 309, 346, 360, 373, 456, 459-461, 466, 468-469, 471, 478
- Contrapesos xvi, 20, 93, 187, 345, 491
- Contratistas 259-260, 431, 442, 462, 473
- Cooperación (véase Inteligencia)
- Coordinación de inteligencia
- Interagencial 8, 11-12, 27, 40, 43, 50, 132, 177, 179, 181, 194, 212, 214, 257, 302, 307, 343, 348, 352-353, 356, 359, 382, 397, 425, 436-438, 492
  - Militar 176, 267
  - Multinacional 270, 280-281, 286-287, 293, 454, 456, 493
  - Corporativismo 138, 320, 332-333, 340
- Corrupción xxxiii, 133-134, 150, 242, 245, 281, 290, 355, 375
- CSIRT (Equipo de Respuesta de Incidentes de Seguridad Informática) 446
- Cuba 7-8, 25, 126, 202, 237-238
- Debate ii, xxvi, xl, 4, 15, 24, 84, 95, 97, 111, 117, 119, 126, 132, 167, 182-183, 191, 212, 246, 270, 318, 322, 324-325, 329, 356, 396, 434, 448, 491, 494-495
- Debilidades 124, 163, 180-181, 212, 222, 224, 255, 302, 403
- Democratización (véase Inteligencia)
- Desclasificación (véase Inteligencia)

- Desinformación 170, 225, 239, 388
- DIDEP (Dirección de Inteligencia del Estado Plurinacional, Bolivia) 23, 355
- DIGICI (Dirección General de Inteligencia Civil, Guatemala) 82, 303, 352
- DIGIMIN (Director General de Inteligencia del Ministerio del Interior, Perú) 43, 46, 84, 352
- Dignidad 151-152, 156, 163, 298
- DINACIE (Dirección Nacional de Inteligencia del Estado, Uruguay) 209
- DINI (Dirección Nacional de Inteligencia, Perú) 3, 10, 13, 16-17, 19, 25, 40-73
- DINIE (Dirección Nacional de Inteligencia Estratégica, Perú) 10, 13
- Diplomado 390, 393-395, 397-400, 407
- DISIP (Dirección de los Servicios de Inteligencia y Prevención, Venezuela) 7, 23, 234
- Divulgación xxi, 33, 37, 191, 365, 486
- DNI (Dirección Nacional de Inteligencia, varios países) 22, 83, 134, 209-210, 303, 437
- DNII (Dirección Nacional de Información e Inteligencia, Uruguay) 209
- DNISP (Doctrina de Inteligencia para la Seguridad Pública, Brasil) 303, 324
- Doctrina (véase Inteligencia)
- Doutrina (véase Inteligencia)
- Ecuador 5, 22, 74, 80, 118, 134, 136, 147, 207, 211-212, 225, 236, 282, 284, 352, 356, 396, 401, 411
- Educación (véase Inteligencia)
- Eficacia xvii, xix, xxii, 22, 87, 109, 124, 136, 144, 196, 215, 250-255, 257, 267, 271, 298, 301, 307, 309-310, 314, 317, 337, 339-341, 363, 391, 455, 490
- Eficiencia xxi-xxii, xxix, xl, 22, 32, 87, 94-96, 109, 127, 132, 177, 183-184, 196, 202, 238, 250-255, 267, 270-271, 307, 317-318, 375, 391, 403-404, 490-491
- Egmont, Grupo xxvii, 244

## Gestión de Inteligencia en las Américas

Ejecutivo (véase Poder)

Endogrupo 158-159

Equipo

de análisis 177, 195, 233

de asesoramiento 375, 430, 436, 446, 453-454, 473-478, 482

de inteligencia económica 227, 242-243

de trabajo 159, 211, 224, 246, 383-384, 388

Error xxix, 11, 13, 18, 125, 127, 153, 228, 236, 413-414, 491

Escenario xxx, xxxvi, 26, 146, 155-157, 164, 173-175, 178-181, 184, 195, 204, 208, 210, 216, 218, 221-222, 227, 287-289, 292, 364, 368, 374-375, 377, 425, 440-443, 445-447, 466

Escuchas xviii, 133, 149, 202, 279

ESG (Escuela Superior de Guerra, varios países) 410, 411

ESICI (Escuela de Inteligencia y Contrainteligencia, Colombia) 395, 411

ESINT (Escola de Inteligência, Brasil) 115, 393, 411

ESISEN (Escuela de Inteligencia para la Seguridad Nacional, México) 398, 399, 411

ESMADE (Estado Mayor de la Defensa, Uruguay) 209

Espionaje xxi-xxii, 12, 120, 125, 128, 133-134, 138, 169, 195, 202, 209, 224-225, 233, 238-239, 246, 278, 425, 428, 430

Estados Unidos xv, xxviii, xxix-xxx, 3, 7, 74, 81, 117, 119-121, 123-126, 130, 132, 141, 146, 160, 164, 197, 249, 257, 262, 268, 271, 280, 283, 297, 299, 319, 327, 348, 362, 396, 401, 411, 425-451, 455, 469, 473, 486, 496

Estrategia xviii, xxxviii, 33, 42, 178, 184, 192, 209, 214, 217, 228, 245, 257, 283, 348, 357, 359, 363, 367, 384, 388, 399-400, 404-405, 435, 446, 453-454

Ética (véase Inteligencia)

Etnicidad 458, 467-468, 470

- Europa 3, 10-11, 14, 100, 121, 129, 131-133, 139, 197-198, 208, 276, 280, 283, 344, 492
- EUROPOL (Oficina de Policía Europea) 276, 285, 304-305, 311
- Evaluación xxiii-xxiv, xxvi-xxvii, xxix, 28, 51, 78, 83, 161, 184, 194, 196, 206, 210, 216-217, 221, 224, 226, 228-229, 231-232, 243, 245, 254, 262, 349, 377, 391, 395, 401, 403-408, 410, 412-416, 420-422, 434-435, 448, 459, 468, 474, 478, 484
- Evidencia xxv, 3, 11, 18, 100, 105, 133, 162, 189, 205, 221, 232, 234, 238-239, 241, 256, 272, 294, 327, 330, 373, 377, 383, 442
- Evolución xli, 5, 7-9, 19-20, 24, 137, 143, 175, 182-183, 189, 205, 215, 217, 228, 231, 285-286, 301, 329, 363, 367, 376, 406, 458, 464, 486, 490
- Externa (véase Inteligencia)
- Facebook xxxviii, 448
- FARC (Fuerzas Armadas Revolucionarias de Colombia) 136, 205-207, 211, 231, 236
- FBI (Buro Federal de Investigación, Estados Unidos) xxxiv, 146, 153-154, 157, 160, 163, 358, 427, 433, 436-437
- Federal xiv, xxix, xxxi, xxxiii-xxxiv, 4, 81, 86, 103-104, 107-108, 115, 124, 128-129, 202, 302-304, 306, 313-314, 320-322, 327, 332, 337, 341, 351, 358, 370, 374-376, 393, 396, 427, 436-438, 445, 448-449, 484
- Financiera (véase Inteligencia)
- Fiscalización (véase Inteligencia)
- FLACSO (Facultad Latinoamericana de Ciencias Sociales) 74
- Fracaso (véase Inteligencia)
- Francia xxvii, 124, 148, 152, 164, 208, 280, 401
- Fronteira 328, 332
- Frontera xxviii, 78, 211, 213-214, 222-223, 228-229, 274, 365, 370, 495
- Fuerzas armadas

## Gestión de Inteligencia en las Américas

- y derechos humanos 136, 302
- y inteligencia xxxvii, 6, 8, 12, 18, 24, 30, 78, 83, 87, 118, 120, 154, 212, 274, 285, 313, 355, 393-394
- Fujimori, Alberto xvii, 10-12, 19, 23
- GAFILAT (Grupo de Acción Financiera de Latinoamérica) 197, 283-284
- Gendarmería xxx, 305-306, 350-351
- Geopolítica 193, 410
- Gerencia 4, 92-93, 98-99, 229, 255-256, 317, 339, 414, 456
- Gestionar xvi, xxxvii, 189, 357, 360, 439-440
- Globalización xxvi, 173, 175, 184, 189, 196-198, 213, 222-223, 290, 489
- Gobernabilidad(e) 29, 86, 174, 218, 317, 329, 339, 341, 345-346
- Grabación 149, 300
- Guatemala 14, 20, 82, 118, 283, 300, 303, 352, 356, 397, 411
- Guerra
  - Contra terrorismo xxix, 9, 121, 123-124
  - Económica 244, 246
  - Fría 7-8, 10-11, 14, 121, 124, 175, 270, 280, 327, 335, 363, 369
  - No convencional 7
  - Subversiva 6, 9, 137, 152
  - Sucia 156-157
  - Tiempos de xiv, 124
- Guerrillero 136, 211, 237
- Guyana 282, 284
- Hacer cumplir la ley (law enforcement) 123, 149, 437-438
- Halcón xxxiii, 372
- HUMINT (Inteligencia de Origen Humana) 26, 210, 211, 215-216, 218, 363
- IAEE (Instituto de Altos Estudios Estratégicos, Paraguay) 209, 399

- Identidad(e) 66, 67, 125, 149-150, 157-160, 163, 238, 297, 310, 333, 365, 377, 427-428, 431, 434, 443, 484
- IIFA (Instituto de Inteligencia de las Fuerzas Armadas, Argentina) 393, 411
- Ilícito 206-207, 213-214, 221-222, 228-230, 244, 371
- Impunidad(e) xxxiii, 4, 138, 145, 150, 364
- Incertidumbre 141, 148, 157, 187, 203-204, 217, 230, 425, 433
- Independiente/independente (véase Inteligencia)
- Indicador xiii, xx, xxviii, 90, 196, 403, 468
- Infraestructura 221, 243-244, 288, 345, 357, 389, 426-427, 430, 434-436, 446
- Injerencia 132, 149, 234, 237-238, 241, 298, 389
- Institucionalidad(e) 176-177, 181, 317, 329, 356, 491
- INSYDE (Instituto de Seguridad y Democracia, México) 378
- IntCen (Centro de Inteligencia, Unión Europea) 278-279, 288
- Integración (de inteligencia) ix, xxix, xxxvi-xxxix, xl, 77, 123, 193, 198, 278-279, 281, 287, 304, 351, 356, 370, 374, 379, 381-384, 391, 490, 494, 496
- Inteligencia
- Agente de xxxii, 93, 96, 121, 124-126, 128-129, 146, 149-154, 163, 211-212, 233, 239, 271, 300, 326, 333-334, 367, 387
  - Autonomía de xv, xx, xxii, xxxv, 5, 17, 48, 61, 127, 151, 177, 186, 190, 303, 308, 332, 334, 355, 361-378, 475, 483, 486
  - Bolivariana 23, 402
  - Burocracia de 99, 170, 179-181, 183-184, 256, 386-387, 391, 448, 454
  - Civil ix, xiii, xxxvii, xl, 5-6, 11, 20, 22-23, 37, 64, 67, 82-83, 85-87, 110, 120, 134, 177, 179, 210, 245, 303, 352-354, 359, 364, 368-369, 393, 398
  - Colaboración en xx, xxix, xxxv-xxxvi, xxxix, xl, 241, 277, 311, 356, 358-359, 364, 372, 381, 383-384, 393, 438

## Gestión de Inteligencia en las Américas

- Como Servicio Público 4, 7, 131-133, 491
- Confiable ix, xxii, xl, 167, 176, 180-181, 214, 233, 313, 370, 378, 404
- Cooperación en xx, xxx, xxxvi-xxxvii, 40, 51, 57-58, 74, 128, 131, 133, 182, 194, 196-198, 211-216, 218, 244, 257, 269-294, 304, 307-311, 344-347, 353, 399, 475-476, 492-495
- Democratización de 131, 191, 201, 344, 409, 489
- Desclasificación y 36-39, 366
- Doctrina de xv, 6, 9, 44, 51-52, 132, 156, 159, 185, 203, 219, 224-225, 232, 246, 302-305, 311, 409, 458, 465, 469
- Doutrina de 3, 317, 322-324, 326-329, 334, 336-338, 340
- Educación en xxxvi, xxxviii, xl, 190, 267, 291, 381-423, 494
- Ética en ix, xix, xxii, xxiv, xxxvii-xxxix, 1, 3, 4, 12, 87, 93, 96, 121-164, 169, 190, 207, 221, 226, 250, 277, 335, 365, 367-369, 377, 383, 385-386, 447, 477, 484, 491
- Externa xxii, xxxix, 49, 79, 83, 96, 101, 105, 110, 114, 130, 197, 227-230, 255, 287, 317, 321, 350, 362, 366, 435
- Financiera xiv, xxiv, xxvi-xxvii, 17, 57-58, 61, 69, 83, 168, 197, 225-248, 263-268, 282
- Fiscalización de xvi, xx, 1, 5-170, 387, 490
- Fracaso de xxxvii, 130, 153, 157, 302, 482
- Independiente/Independente 83, 145, 195, 235-236, 252, 355, 365, 368
- Limitaciones de 204, 269-294, 298, 307-309, 313, 407, 414, 420, 466, 472
- Militar xvii, xxxv, xxxvi, 6, 8, 22, 28-29, 40, 46, 80, 115, 119-120, 137, 175, 177, 240, 259, 274, 282-283, 286-287, 292, 302, 304, 328, 351-354, 363, 368-369, 373-374, 396, 402, 437-438, 441, 472
- Multilateral xxvii, xxvi, 41, 45, 84, 137, 213, 215, 269-294, 310, 362, 425-486, 492-493, 496



## Russell G. Swenson y Carolina Sancho Hirane

- Operacional xiv, xxii, xxxii, 76, 121, 171, 232, 243-244, 275, 317, 334, 338, 401, 442, 468, 472
- Penitenciaria 305-307, 343-360, 494
- Policial xxviii, xxix-xxv, 10, 22, 28-29, 40, 80, 85, 117, 163, 168, 177, 215, 274, 282-283, 285-294, 303-305, 326-327, 330, 336, 344, 348, 351-360, 370, 381, 493-494
- Preventiva xviii, xxxii, xxxviii, 33, 152, 168, 214, 232, 239, 269, 274, 288, 314, 330, 338, 346, 374
- Profesionalismo de xvi, xx, xxxiv, 163, 169, 177, 181-183, 191, 248, 272, 290, 361-362, 408, 458, 468
- Recolección y xix, xli, 14, 19, 23, 26, 28, 78-79, 120, 129, 150, 190, 194, 224, 239, 260, 279, 349-350, 370-371, 373-374, 377, 435, 438, 471
- Recopilación y xxix-xxxi, xxxiv-xxxv, xxxviii, 190, 195, 314, 450, 464, 473
- Requerimientos de 243, 264, 270, 355, 388, 410, 434, 447, 457, 463, 472-474, 476-477, 490, 492
- Seguimiento y 21, 117, 120, 131, 146, 148, 152, 202, 216, 239-240, 244, 266, 271, 288, 299
- Socia xxxv
- Teoría de 195, 221, 224, 226-227, 233, 270, 273, 356, 409
- Transformación de 132, 144, 222, 381, 462
- Transmisión de 222, 224, 227, 236-238, 243-244, 361-362, 385
- Interagencial 10-12, 177, 181, 194, 212, 215-216, 218, 270, 494
- INTERPOL (Organización Internacional Criminalística de Policía) 283, 304, 401
- Interrogación 152, 374
- Intrusivo (véase Inteligencia)
- Investigador 129, 170, 246-247, 372, 398, 440
- Irak xiv, 121, 123, 127, 271, 475

## Gestión de Inteligencia en las Américas

- ISAF (Fuerza Internacional de Apoyo, Afganistán) 383, 457-458, 472-473
- Israel xxiii, 124, 128, 410
- Italia 109, 164, 208, 280, 304
- Jefatura 9, 79, 263
- Judicial (véase Poder)
- Lealtad xxvii, 158, 237-238, 386, 430, 458
- Legalidad(e) xxii, 32, 58, 97, 99, 109, 113, 127, 129, 148, 154, 163, 169, 223, 329, 490, 494
- Legislativo (véase Poder)
- Legitimidad(e) xx, xxii, 3, 32, 133, 141, 147, 160, 173, 180, 298, 307, 317, 327, 337, 455, 491, 494, 496
- Liderazgo xvii, 140, 228, 230, 255-256, 263, 294, 305, 344, 459, 462, 473-474, 478, 480, 490
- Limitaciones (véase Inteligencia)
- LULZSEC (grupo hactivista) 431-433
- Manejo xvi, xxvii, xxxiv, 13, 18, 34, 36, 150, 168, 174, 177, 183, 190, 196, 202, 231, 250, 264, 278, 293, 383, 389, 425-427, 435, 444, 462, 472, 477, 483
- Medir 180, 196, 232, 238, 251-253, 262, 266-267, 314
- MERCOSUR (Mercado Común del Sur) 197-198, 275, 284-285, 292
- Mercyhurst University 397
- Metodología xii, 173, 179, 181, 189, 205, 216, 218, 304, 394, 399, 491
- México xiii, xxviii, xxxii-xxxv, 20, 85-86, 118, 134, 147, 167, 169, 206, 213, 215, 274, 313-314, 372-375, 378, 398, 411
- Militar (véase Inteligencia)
- Monitorear xxxvi, 202, 242, 348-349, 437, 441, 447, 459
- Montesinos, Vladimiro 11-13, 19, 23
- Moralidad 122, 161
- Multilateral (véase Inteligencia)

**Russell G. Swenson y Carolina Sancho Hirane**

- Multinacional xv, 233, 271, 273-274, 284, 310-311, 453-456, 471-472, 483, 486
- Nepotismo 133
- Neutralizar xx, 90, 177, 193, 208, 243, 322, 396, 408
- Nicaragua 119, 207, 300, 353
- Obediencia debida 135
- OEA (Organización de los Estados Americanos) 12, 206, 276, 347, 400-401
- Operacional (véase Inteligencia)
- Oportunidad xiv, xv, xviii, xxii, xxiv, xxvi, xxviii, xxxii-xxxv, xxxviii, xl, 11, 28, 31, 42, 89, 136, 139, 167, 174, 176-177, 183, 192, 195, 204, 213, 215, 218, 224, 228, 233, 235, 242, 263, 271, 273, 281, 284, 290, 293, 297, 311, 317, 350, 356, 361, 367, 386, 397, 409, 420, 435, 439, 460-461, 463, 474, 480
- OSINT (Inteligencia de Fuentes Abiertas) 216
- OTAN (Organización del Tratado del Atlántico Norte) 133, 197, 278, 280, 363, 453, 455-456, 472, 481
- Pandillas 348-349
- Paradigma xxxi, 188, 219, 246
- Paraguay 87, 119, 193, 205, 208, 213-214, 282, 284, 399-400, 411
- Peligro xiii, xvi, xxxiii-xxxiv, 14, 17, 19, 32, 60, 63, 68, 168, 204, 207, 218, 224, 228, 269, 277, 355, 363, 366, 375, 389, 425, 445, 475
- Penal xxxv, 37, 53, 55, 64, 67, 107, 137, 155, 224, 232, 301, 306, 308, 311, 314, 331, 334, 345-346, 349, 352, 357, 359
- Penitenciaria (véase Inteligencia)
- Perfil 10, 11, 21, 72, 179, 194, 214-215, 233, 240, 244, 257, 260-262, 291, 322-323, 390, 410
- Periodistas xxiv, 9, 14, 123, 128, 134, 138, 140, 202
- Personal (véase Inteligencia)

## Gestión de Inteligencia en las Américas

Persuasivo xxv, 139

Perú xvii-xviii, xxviii, 3, 5-73, 83, 119, 134, 147, 169, 205-206, 210, 213,  
282, 284, 352, 400-401, 408, 411

Plurinacional 23, 355

Poder

Ejecutivo xvi, xxii, xxviii, 5, 9, 12, 15, 25, 56, 143, 146, 190, 213,  
217, 269, 353, 355, 439, 450

Judicial xvi, 16, 56, 61-62, 71, 117-119, 132, 183, 203, 306, 346,  
350, 359-360, 387

Legislativo xvi, xviii, 18, 56, 90, 92, 94-95, 102, 105, 107-108, 110,  
117-119, 187, 203

Policial (véase Inteligencia)

Portugal xviii, xix, xxxv, 110

Prácticas (de inteligencia) ix-xi, xiii, xviii, xxi-xxii, xxv, xxxix, 18, 122-123,  
128, 132-134, 138-139, 145, 148, 150-152, 155-157, 160,  
164, 169, 177-178, 183, 189-190, 196, 201, 205, 223-226,  
230-231, 239, 241, 244-245, 249-250, 266, 269, 273, 275-  
276, 280, 282, 314, 361, 364, 367, 320, 377, 405, 426,  
446-447, 475, 490, 494, 496

Prensa xxi, 93, 97, 127, 140, 168, 232, 348, 425, 449

Prestigio xx, 137, 180, 226, 279, 328, 390

Preventiva (véase Inteligencia)

Principios

Cooperativos 277-278

Doctrinarios de inteligencia 15, 23, 87, 98-100, 185, 241, 249-250

Éticos de inteligencia xx, 121-165, 493

Legales de inteligencia xix, xxi, 27, 32-33, 84, 92, 344, 353

Parlamentarios de inteligencia 19, 23

Presupuestales 263-266

## Russell G. Swenson y Carolina Sancho Hirane

- Privacidad xvi, xxviii, xxxviii, 118, 129, 133, 140, 149, 295, 297-301, 339, 447-448, 450, 490-491, 493
- Profesionalización (véase Inteligencia)
- Prospectiva xxiv, xxvii, 209, 218, 381, 388, 395, 401, 441
- Psicológico xv, xxv, 51, 148, 155, 161-163, 179, 381, 402
- RCMP (Real Policía Canadiense Montada) 111-112
- Reciprocidad(e) 162, 332, 334
- Reclutamiento 179, 239, 370, 386
- Recolección (véase Inteligencia)
- Recopilación (véase Inteligencia)
- Rendición de cuentas (Accountability) xvii, xxi, 8, 15, 20-22, 48, 59, 73, 121, 129-130, 238, 250, 356, 361-362, 366-367, 369-373, 377-378, 494, 496
- Represión 136, 144, 191, 306-307, 319
- Requerimientos (véase Inteligencia)
- Revanchismo 102
- RILO (Oficina Regional de Enlace de Inteligencia) 197, 244, 283-284, 290, 292
- Salvaguarda 95, 101, 106, 109, 111, 123, 318, 362, 408
- SEBIN (Servicio de Inteligencia Bolivariano, Venezuela) 23, 87, 202, 402
- Secretismo 150, 311
- Seguimiento (véase Inteligencia)
- SENAIN (Secretaría Nacional de Inteligencia, Ecuador) 22, 136, 212, 396
- SENASP (Secretaria Nacional de Segurança Pública, Brasil) 302-303, 321, 323
- Sinergia 247, 338, 370, 449
- SNBAT (Equipo de Red Socio-política y Análisis de Comportamiento) 453-486

## Gestión de Inteligencia en las Américas

Social (véase Inteligencia)

Sociedad(e)

Civil xviii, 140, 195, 202, 246-247, 249, 457, 480

del conocimiento xiii

STASI (Ministerio de Seguridad del Estado, República Democrática de Alemania) 10, 14, 145, 149

Supervisar 22, 50, 190, 249, 279, 351, 366, 402, 436

Supervivencia 143, 162, 221, 224, 239

Supranacional 279-280, 366

SURNET (Red Sudamericana de Comunicaciones Protegidas) 197, 283, 286, 292

Tecnología 189, 222, 227, 333, 335, 338, 377, 381, 396, 426-427, 430, 434, 493

Tensiones xvi, xxii, 25, 124, 133, 270, 278, 349, 370-371, 493

Teoría (véase Inteligencia)

Territorio xiv, xxii, 8, 76, 86, 101, 136, 143, 159, 213, 236, 291, 308, 333, 335, 368, 370

Terrorismo

Financiación de 69-70, 225, 244, 283

Lucha contra xxix, 9-10, 81, 111, 119, 121, 123-129, 146, 205, 276-278, 281, 311-312, 331, 369-371

Testigos 5, 150, 152, 376

Tortura 121, 123, 128-129, 135, 145, 152-160, 163, 308, 370

Transformación (véase Inteligencia)

Transmisión (véase Inteligencia)

Transparencia xix, 13, 15, 20-21, 34-35, 72, 87, 89-90, 97, 103, 107, 129, 132, 190, 202, 356, 365, 371, 373, 408, 490, 491

UNASUR (Unión de Naciones Suramericanas) 182, 196-198, 269-294, 312, 493

**Russell G. Swenson y Carolina Sancho Hirane**

- Uruguay 5, 22, 84, 87, 119, 193, 198, 209, 212-214, 282, 284, 355-356, 401, 411
- Validez 122, 150, 289, 367, 377
- Venezuela 5, 7, 23, 87, 147, 202, 205, 207, 225, 227, 229, 234-238, 240-241, 282, 284, 401-402, 411
- Verificar 85, 112, 299, 392, 406
- Vigilancia xv, xviii, 91, 120, 146, 148, 152-153, 228, 231, 238, 241, 247, 249, 299, 305, 400
- Vulnerabilidad(e) xxxi, xxxviii, xl, 14, 29, 94, 157, 159, 221, 235, 271, 273, 281, 335, 366, 433, 490
- Wikileaks 432, 462, 471





Ao focalizar no gerenciamento da inteligência e ao reunir as análises de autores altamente respeitáveis, esta peça revela nuances normalmente despercebidas em prévias publicações. Além disso, o livro é especialmente dramático ao revelar a incongruência entre algumas das organizações de inteligência existentes e a norma democrática. Por essas razões, este livro estimulará e refinará o debate com vistas ao aperfeiçoamento da democracia na região.

**Dr. Luis Bitencourt,**

Professor e Decano de Assuntos Acadêmicos do Perry Center/National Defense University

Esta coleção de ensaios oferece ao leitor uma completa visualização da trajetória histórica institucional da inteligência em muitos países da América Latina. Ao mesmo tempo, os trabalhos destacam os desafios atuais que enfrentam representantes políticos e funcionários do governo ao buscar melhorias desta função em estados democráticos. Um ensaio em particular ilustra uma novidade ao examinar a expansão da concepção tradicional de inteligência e a sua conduta em apoio ao governo dos Estados Unidos, destacando uma inovadora experiência de campo na compreensão sociopolítica local num contexto de aconselhamento militar numa missão no estrangeiro.

**Dr. Thomaz Guedes da Costa,**

College of International Security Affairs, National Defense University, Washington, DC

En democracia la actividad de inteligencia es más necesaria que nunca, precisamente porque debe proteger la institucionalidad de quienes no creen en un sistema de libertades donde todos puedan participar sin cortapisa alguna. En ese contexto, la función de recabar información debe tener un sentido. La función de inteligencia fue abusada y usada con fines perversos durante los regímenes dictatoriales que han asolado la región. Lo anterior ocasionó que muchas democracias nacientes tuvieran poco celo e interés en el tema, cuestión que se ha ido subsanando lenta y progresivamente. Este libro ayuda a disimil evolución en la materia. La diversidad de casos y realidades presentadas nos obliga a pensar en siguientes pasos, tales como las estandarizaciones internacionales en materia de uso y control de inteligencia. Este es un texto que ayuda a comprender cómo los Estados tienen que enfrentar la función de inteligencia desde una realidad empírica compleja.

**Dr. Jaime Baeza Freer,**

Instituto de Asuntos Públicos, Universidad de Chile

Valiosa aportación para la comprensión de la inteligencia en el área latinoamericana. Junto con agradecer el valor de la comparación, el texto abre nuevos espacios de reflexión como la ética, el papel de las comunidades de inteligencia o el ámbito penitenciario y la relación entre seguridad pública e inteligencia. Esta obra colectiva tiene el gran mérito de reunir a un selecto grupo de expertos para, evitando redundancias, abordar temas, algunos de ellos de indudable valor seminal de los cuales los lectores experimentados sabrán disfrutar.

**Dr. Antonio Díaz**

Universidad de Cádiz, España

La supervisión y el control de los servicios de inteligencia en una democracia, bajo una clara regulación jurídica, es una exigencia para garantizar el cumplimiento por estas instituciones de su función estatal de un modo respetuoso con la legislación vigente y los derechos y libertades de los ciudadanos. Y también es una garantía para los propios servicios de inteligencia de que la supervisión y el control indican los límites por medio de la: indicación de objetivos, dotación y dirección de medios y derecho a pedir rendimientos de cuentas sobre sus resultados y métodos, para evitar así su intervención para intereses particulares o un uso partidista. Este libro, que reúne colaboraciones de 20 autores, pasa revista al estado actual y a los principales retos de una función clave para la seguridad nacional y la consolidación de los regímenes democráticos.

**Dr. Miguel Ángel Esteban,**

Universidad de Zaragoza, España

ISBN 978-1-932946-44-4

9 0000 >



9 781932 946444

