NATIONAL INTELLIGENCE UNIVERSITY

Ann Caracristi Institute For Intelligence Research

What this is:

This report is the product of academic research. As the IC's university, NIU is uniquely positioned to use academic approaches to research—and report on—subjects of interest to the community.

What this is not:

This is not finished intelligence. The opinions expressed in this report are solely the author's and not those of the National Intelligence University or any other U.S. Government agency.

RESEARCH SHORT

CATALYST Designed to spark positive conversations on the future of the IC

June 23, 2021

IMAGE FROM SHUTTERSTOCK

From a Whisper to a Shout: The IC Should Use Its Outside Voice

Debora Pfaff and Bowman Miller

National security is the U.S. Government's most basic responsibility, laid out in the first sentence of the Constitution's preamble: provide for the common defense. But what was once the exclusive domain of the public sector now depends on a range of actors, individuals, corporations, and entities who—unlike government—are not beholden to the public interest. Their voices are noisy, voluminous, and—because they know little about how the government protects them and even less about the role of the Intelligence Community in national security—often ill-informed. Their increased willingness to challenge government authorities means that, unless the IC finds its voice within this rising cacophony, its silence will facilitate its demise and, along with it, the safety and security of the nation it is sworn to protect and defend.

For more than two centuries, the defense of the nation has depended on its ability to command physical domains—air, land, sea, and, most recently, space. Securing these domains involved a relatively straightforward identification of adversaries, followed by an evaluation of their intent and capabilities. Although surprises did occur, they were mostly within the realm of identified plausibility.

This, quite simply, is no longer the case. A fifth domain—cyberspace—has democratized the array of potential actors and threats. A mere two decades into its existence, the nation is now uncertain who may be in a position to cause it harm, whether they intend to be adversarial in the first place, and how their actions in the virtual domain will impact the four physical domains. The tremendous increase in the type and number of actors able to participate in—and control—the cyberspace domain means power can shift from the relatively large institution of government to a single individual.

Consider a few examples. Twitter censored then-President Trump after the January 6, 2021, attack on the U.S. Capitol, citing concerns about "the risk of further incitement of violence."[1] Critics have decried Twitter's ban as coming from a private entity wielding disproportionate power to quash free speech, while supporters argue Twitter is its own company, free to set its own rules. Elsewhere, Australia has demanded that tech giants like Facebook pay for the nation's news, and in response Facebook banned all Australian news on its site.[2] The hacktivist group Anonymous—deemed freedom fighters delivering extrajudicial justice by those who like them and cyber-terrorists by those who do not—has conducted numerous cyberattacks against government institutions and private corporations across the world. Finally, a decade ago an ordinary Tunisian street vendor, Tarek el-Tayeb Mohamed Bouazizi, sparked the 2010 Arab Spring with a singular act of self-immolation that galvanized the Arab world through social media.

In all these examples, an individual or private entity undertook actions that temporarily or permanently shifted the balance of power away from a government. That government's ability to regain and retain its eroded power largely depends on its credibility, but earning credibility is no longer as simple as publicizing fact-based information supported by scientific inquiry to arrive at genuine knowledge. Attention has become a resource, and the right to silence a luxury.[3] The twin disruptors of misinformation and disinformation have produced an environment in which an explosion of information—with varying degrees of accuracy—saps the public of the energy to separate what it needs to know from what someone wants it to know. Everyone operates in a new reality informed by a 24-hour news cycle, disproportionately powerful social media, and an excess of information with a low signal-to-noise ratio.

Democracy and democratically accountable institutions like the IC's 18 members require the public to have knowledge, not just faith.

Increasingly, choosing what to pay attention to also means choosing what to believe. As people's brains struggle with information overload, they try to make sense of competing data streams, and in their evaluation, they tend to trust information that fits into their preexisting worldview, which reinforces hardened beliefs.[4] This is especially troubling for national

security because most of what the public hears and believes about national intelligence comes from information sources outside the Community. The IC's voice has not gotten lost in the noise—it was never there in the first place.

Eschewing Public Discourse . . .

From its very beginning, the IC was modeled on and grounded in secrecy. It was forced to mature rapidly as a mechanism to deal with the Soviet Union and quickly evolved into a closed system that required secret collection methods to obtain information on the enemies of the United States.[5] Well before the National Security Act of 1947 officially created the basis for the Community we know today, America's leaders had embraced the value of espionage—of secrecy as the basis for intelligence success.[6] They were not alone: Austria, Britain, France, Germany, Italy, and Russia all established permanent intelligence functions before the United States,[7] and all were steeped in "collect[ing] and classify[ing] all possible information relating to the strength, organization etc. of foreign armies. . . ."[8]

This posture permeated every part of the IC's culture until secrecy became *what* we do, as well as *how* we do it. As a rule, the IC evinces a strong preference for classified over open-source information, at times to the detriment of accuracy and information sharing.[9, 10, 11] Examples of this emphasis on secrecy abound, at costs well beyond financial considerations. CIA's Directorate of Operations has a staff and a budget at least three times larger than that of its Directorate for Analysis.[12] The costs of security classification more than doubled from $8.65 billion in 2007 to $18.39 billion in 2017, the last year the Information Security Oversight Office has reported such figures.[13]

In our eagerness to ensure information does not slip into the wrong hands, we have forgotten that the hand that feeds us belongs to the American public. They are the greatest consumer of the public good that is national security. Democracy and democratically accountable institutions like the IC's 18 members require the public to have knowledge, not just faith.

The IC has made cursory attempts at transparency: creating the **Intel.gov** website; publishing the Principles of Transparency for the Intelligence Community; and launching a handful of Twitter sites and forward-facing agency webpages. However, these efforts have been reactive, not proactive—always in response to an accusation of wrongdoing. They are meant to mollify and slake the public curiosity, rather than to engage and assimilate. The unwillingness to even consider a comprehensive, IC-wide strategy for engaging the public has put the IC back on its heels, forced to defend its position to a skeptical public without offering evidence and without the benefit of an established brand and a proven track record.

Data on the IC is restricted for nearly all of the American public, which must then turn to available sources of information to make sense out of the basic need that is national security. We let others speak for us. Journalists, Congress, political elites, and the entertainment industry form too much of the public's perception of the IC. And each of these entities has its own motivated reasoning for communicating certain information in a particular way, which does not always line up with

the Community's intent and interests. The voices outside of the IC carry, while ours remain behind SCIF doors, firewalls, and steel fences. In the absence of evidence, the impressionable human mind fills in the blanks, using motivated reasoning to believe what it wants to believe.[14] Because the IC cannot talk about our wins, our losses appear to be mounting.

We do not speak because we are terrified that we will say something we should not or will reveal too much . . . or even prove to be *wrong.* This fear of risk has pervaded the IC since the threat-based approach to national security emerged after WWII. The irony of our efforts to avoid public attention by eschewing public discourse is that the IC is now on a collision course with exactly what we want to avoid. We have target fixation. The IC has a strategy for everything but how to engage our most important customer—the American people—and that is going to end with an explosion we are ill-equipped to handle.

. . . Proves Problematic in a Changing World

It is unlikely that a single event will provoke a consequential failure of public confidence in the IC; rather, it is and will continue to be a slow erosion. Recent polling by the Chicago Council on Global Affairs indicates that a majority of Americans believe the IC is effective and necessary.[15] But 78 percent of the Silent Generation approves of the IC, compared with just 47 percent of Millennials. And an already growing perception exists among half of Americans that intelligence agencies sacrifice civil liberties in pursuit of their mission.[16] The proliferation of entertainment industry depictions, which purport that the NSA records every American's phone calls and that everyone who works for the CIA is another James Bond or Carrie Mathison, will continue to mislead, mystify, and misinform. Without authoritative information directly from a trusted IC, Americans will continue to form opinions based on fiction and hyperbole.

The Intelligence Community, like most federal entities, depends on contractors. To serve their government clients, contractors develop the same—or perhaps even better—capabilities. Thus far, the prohibition against contractors serving in inherently governmental roles has prevented a formal shadow IC from forming around these private entities. Contractors cannot undertake any function that is "so intimately related to the public interest as to require performance by federal government employees."[17] During a Senate Homeland Security and Governmental Affairs Committee Hearing on the Intelligence Community Contractor Workforce, Principal Deputy Director for National Intelligence Stephanie O'Sullivan stated that those functions include "decisions on priorities, strategic direction or commitment of resources."[18]

The IC has relied on this policy to preserve the provision of decision advantage to policymakers as an inherently governmental function. What cannot be controlled is where the attention of the policymaker will be directed. In fact, non-intelligence sources have already begun competing for the attention of the policymaker—often with success. A RAND Corporation study found that policymakers valued accuracy and timeliness above all else and were often disappointed by how long it took to receive intelligence from the IC on pressing matters.[19] Policymakers turn to the most available sources, including television, advisors, print

journalism, and the Internet to glean information with which to make a decision paramount to national security. These voices are not beholden to the public interest, and their motivations include influencing U.S. policy and activity.

If there are lingering doubts as to whether private industry could appropriate a mission of the U.S. Government, the April 23 launch of SpaceX is a ready reminder that it is already happening. In 2006, NASA invested in the then four-year-old company in the hope it could provide cargo and crew transportation to the International Space Station (ISS) to reduce NASA's need to purchase seats on Russian flights. Since its first flight to the ISS in 2020, SpaceX has grown into a $2 billion corporation with 1,000 satellites in orbit and designs on populating Mars. This has not gone unnoticed by NASA and has sparked a debate about SpaceX's divided attention between its own ambitions and its NASA obligations.[20]

It Is Time To Speak Up

Intelligence specialist and scholar Amy Zegart suggests the IC has shown that its programs are legal but has not shown that they are valuable.[21] And what the American public does not see while streaming episodes of Alias and reading WikiLeaks is that the Intelligence Community provides the one thing the private sector seldom can: all-source objectivity.

Does this mean opening up our doors to the world and discussing every aspect of our business? Absolutely not. Democracy and security have a tenuous balance. Democracy demands free and open public dialogue about the decisions those elected or appointed are making on behalf of the governed. Security demands just the right measure of discretion to allow the public to provide informed input about the strategic direction of the country, and how its leaders are keeping it safe.

> Both exposure and secrecy are essential to a truly free society. But we must achieve a new theory of secrecy appropriate to our new society of instant communication, universal education, and mass opinion . . . in most cases, 'need to know' would also provide the basis for sharp delineation between the politically significant information needed for public decision making, and the technical detail not essential to such decisions.

Dr. Pfaff and Dr. Miller co-direct NIU's Center for Truth, Trust, and Transparency (Tr3), which explores the IC's complex, changing relationship with the public. The public has relied on the IC for national security but knows very little about how it comes to enjoy that public good. Citizens are now an integral part of the national security mission, and we in the IC have a responsibility to bring them into the fold. This does not mean sacrificing security for transparency . . . but it does mean having some conversations long considered culturally taboo in the IC. Is the Intelligence Community still most effective operating within its current level of secrecy? We do not really know because we are too afraid to ask. And that is exactly why the IC should meaningfully reexamine and assess how it can best be available to the U.S. public while keeping the nation's adversaries at bay. NIU's Tr3 Center aims to pose and research these kinds of questions and to explore options for expanding the scope of IC interaction with the public that it serves to defend and also increasingly to inform.

> The latter generally constitutes the data which would be of value to our nation's adversaries.[22]

William Colby wrote these words in 1976. Thus, the need for increased engagement with the public is hardly new. It has simply been ignored because . . . well, ignoring it was possible. We cannot do that any longer. As others' voices rise to add to the global cacophony, we in the IC must embrace our own conversations within our own walls, conversations that ask questions about building a strategy to engage the public, transparency efforts, our blended commitment to security, a credible voice, and true value to the common defense.

If these conversations do not take place—earnestly, expansively, and soon—the growing privatization of the intelligence function becomes a very real risk. With the seeds already sown, private intelligence companies eventually will compete for policymaker attention, eager to fill in gaps and meet consumer requirements for timeliness, speed, and even accuracy. As trust in their methods and findings grows, the centrality of the official, government IC will diminish. So, we must assume the risk of challenging the IC's beloved raison d'être, tune out the guardians of the status quo, and come to terms with the information-hungry world we have, not the one we might want.

The IC must stop whispering and be heard.

Dr. Deb Pfaff is an Associate Professor of Research with the Ann Caracristi Institute at National Intelligence University. She has 20 years of government service, 17 with the IC. Prior to her time with NIU, she served in the analyst career field at DIA. She holds a Doctorate in justice, law, and criminology from American University, and a master's degree in forensic science from The George Washington University.

Dr. Bo Miller is a Professor of Transnational Issues at the National Intelligence University where he has taught since 2005. His more than 50 years in intelligence have spanned Air Force counterintelligence, Department of State all-source intelligence analysis, research, and teaching. He is a retired Senior Executive with 18 years as Director of Analysis for Europe in State's Bureau of Intelligence and Research, and his research and publications focus on Europe, terrorism, and IC challenges.

If you have comments, questions, or a suggestion for a Research Short topic or article, please contact the NIU Office of Research at **NIU_OOR@dodiis.mil**.

Endnotes

1 "Permanent Suspension of @RealDonaldTrump," *Twitter* (blog), Twitter, Inc, January 8, 2021, blog.twitter.com/en_us/topics/company/2020/suspension.html.

2 Elizabeth Dwoskin and Gerrit De Vynck, "Facebook's Brazen Attempt to Crush Regulations in Australia May Backfire," *Washington Post*, February 19, 2021, www.washingtonpost.com/technology/2021/02/18/facebook-australia-news-publishers-regulations/.

3 Matthew B Crawford, *World Beyond Your Head: on Becoming an Individual in an Age of Distraction* (New York: Farrar, Straus & Giroux, 2016).

4 Janna Anderson and Lee Rainey, "The Future of Truth and Misinformation Online," *Pew Research Center,* October 19, 2017, https://www.pewresearch.org/internet/2017/10/19/the-future-of-truth-and-misinformation-online/.

5 Josh Kerbel, "The U.S. Intelligence Community's Kodak Moment," *The National Interest*, May 14, 2014, nationalinterest.org/feature/the-us-intelligence-communitys-kodak-moment-10463.

6 "From George Washington to Colonel Elias Dayton, 26 July 1777," *Founders Online,* National Archives, https://founders.archives.gov/documents/Washington/03-10-02-0415. [Original source: *The Papers of George Washington*, Revolutionary War Series, vol. 10, *11 June 1777–18 August 1777*, ed. Frank E. Grizzard, Jr. (Charlottesville: University Press of Virginia, 2000), 425–26].

7 Christopher Andrew, *The Secret World: A History of Intelligence* (New Haven: Yale University Press, 2018).

8 Thomas G. Fergusson, *British Military Intelligence, 1870-1914: The Development of a Modern Intelligence Organization* (London: Arms and Armour Press, 1984), 45.

9 Roderick M. Kramer, "A Failure to Communicate: 9/11 and the Tragedy of the Informational Commons," *International Public Management Journal* 8, no. 3 (2005): 397-416, https://doi.org/10.1080/10967490500439867.

10 James M. Davitch, "Open Sources for the Information Age: Or How I Learned to Stop Worrying and Love Unclassified Data," *Joint Forces Quarterly* 87 (2017): 18–25.

11 Cortney Weinbaum, "The Intelligence Community's Deadly Bias Toward Classified Sources," *Defense One,* April 9, 2021. https://www.defenseone.com/ideas/2021/04/intelligence-communitys-deadly-bias-toward-classified-sources/173255/.

12 Gregory F. Treverton, *Reshaping National Intelligence in an Age of Information* (Cambridge: Cambridge University Press, 2008), 146.

13 "Information Security Oversight Office, 2017 Report to the President," National Archives Records Administration, https://www.archives.gov/files/isoo/reports/2017-annual-report.pdf.

14 Kirsten Weir, "Why We Believe Alternative Facts: How Motivation, Identity and Ideology Combine To Undermine Human Judgment," *Monitor on Psychology*, American Psychological Association, May 2017, www.apa.org/monitor/2017/05/alternative-facts.

15 Stephen Slick et al., "Annual Polling Confirms Sustained Public Confidence in U.S. Intelligence," *Lawfare* (blog), July 10, 2019, www.lawfareblog.com/annual-polling-confirms-sustained-public-confidence-us-intelligence.

16 Stephen Slick and Joshua Busby, "2019 Public Attitudes on US Intelligence," *Chicago Council on Global Affairs*, September 4, 2020, www.thechicagocouncil.org/research/public-opinion-survey/2019-public-attitudes-us-intelligence.

17 Section 5 of Federal Activities Inventory Reform Act of 1998, PL 105-270, codified at 31 USC 501 (1998).

18 Elaine Halchin, "The Intelligence Community and Its Use of Contractors: Congressional Oversight Issues," U.S. Congressional Research Service R44157, August 18, 2015.

19 Lorna Teitelbaum, "The Impact of the Information Revolution on Policymakers' Use of Intelligence Analysis" (PhD diss., Pardee RAND Graduate School, 2005), 205.

20 Kenneth Chang, "After Sparring, NASA and SpaceX Declare a Shared Mission," *New York Times*, October 10, 2019, www.nytimes.com/2019/10/10/science/nasa-spacex-elon-musk.html.

21 Amy Zegart, "Real Spies, Fake Spies, NSA, and More: What My 2012 and 2013 National Polls Reveal," *Lawfare* (blog), October 2019, www.lawfareblog.com/real-spies-fake-spies-nsa-and-more-what-my-2012-and-2013-national-polls-reveal.

22 William E. Colby, "Intelligence Secrecy and Security in a Free Society," *International Security* 1, no. 2 (1976): 3-14, https://doi.org/10.2307/2538496.