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

December 7, 2022

IMAGES FROM PLANETSCOPE, https://api.planet.com/gallery/v1/posts/forest-fires-near-rubizhne

Integrating Nonstate Intelligence: Ukraine Shows How It Might Work

Thomas Ewing

The war in Ukraine has seen nonstate actors, including private corporations and NGOs, assume a prominent role collecting, producing, and distributing intelligence—directly impacting military operations. Although these "intelligence auxiliaries" have helped Ukraine defend itself, the absence of an overall coordinating mechanism for interoperability with state actors presents a risk that state and nonstate actors will find themselves at cross purposes on the battlefield. Today, the United States and its allies have an opportunity to structure interactions with intelligence auxiliaries under a durable, legal framework with a division of labor that can ensure nonstate intelligence actors contribute effectively to IC priorities in future fights.

The War in Ukraine Demonstrates the Power of Nonstate Intelligence Auxiliaries

The war in Ukraine is revealing what many have known for a long time: open-source intelligence (OSINT) tools and tradecraft have fundamentally changed how intelligence work is done—and by whom. Throughout the conflict, nonstate actors have engaged in classic intelligence operations, from data collection and analysis to influence operations and tactical battlefield intelligence, surveillance, and reconnaissance (ISR). Examples have littered the headlines since the war's beginning: for instance, Starlink, a commercial satellite infrastructure, is supplying Ukraine with both strategic and tactical information, as well as reliable internet connection.[1, 2] Closer to the ground, the widespread use of consumer drones by non-governmental organization (NGO) volunteers has enabled the Ukrainian army to significantly boost its capability for tactical ISR,[3] while nonstate actors using open-source information are contributing intelligence to targeting decisions—on both sides of the conflict.[4, 5]

Many advanced capabilities are being fielded in a conflict of this scale for the first time, often by nonstate actors.[6, 7] For instance, commercial artificial intelligence has been able to sift through immense volumes of intercepted Russian radio communications to create a database of Russian commanders' orders—and thus an archived and searchable record of their plans.[8] Corporations have been able to activate remote kill switches on stolen farm equipment—helping track the provenance of the Russian units that pillaged it.[9] Facial recognition software donated to Ukraine by foreign corporations is allowing individual Russian soldiers who are suspected of atrocities to be identified out of entire units—and potentially singled out for war crimes tribunals. Meanwhile, atrocity crime databases are also being curated by nonstate volunteers from around the world asynchronously using modern communications software.[10]

Off the battlefield, Ukraine has deliberately cultivated relationships with nonstate actors to enhance its intelligence and information operations efforts. The Ukrainian state and other hacktivist actors have released troves of Russian data to the wider world, allowing freelance actors globally to attack Russia in the cyber and information domains.[11] This has at times taken creative forms—in one example from early in the conflict, enterprising programmers have designed tools to degrade Russia's wartime capability and simply waste the Ministry of Defense's time by saturating their phone

KEY RESEARCH INSIGHTS

- Nonstate intelligence actors or "intelligence auxiliaries" are using OSINT tools and tradecraft to have an impact on the course of the conflict in Ukraine—across the entire spectrum of traditional intelligence gathering and analytical activities.
- Although Ukraine has effectively leveraged these emerging intelligence auxiliaries in its immediate fight against Russia, neither Ukraine nor the United States is working toward a long-term framework for state collaboration with nonstate intelligence actors.
- Without coordination, intelligence auxiliaries will continue to act on their own, creating a risk of harming friendly intelligence efforts, violating civil liberties, contributing to misinformation, duplicating work done by state actors, or increasing friendly counterintelligence risk.
- The United States has an opportunity to learn from the ongoing conflict in Ukraine and develop its own framework for successful collaboration with intelligence auxiliaries. A conceptual framework could aid in maximizing the benefits and minimizing the costs of ongoing nonstate intelligence activity into the future.

lines.[12] Nonstate actors are also contributing to strategic-level targeting decisions off the battlefield: although NGO actors have long been consulted in the nomination of individuals or companies for state sanctions enforcement,[13] this engagement is stepping up under Ukraine sanctions programs, giving nonstate actors a prominent role in important sanctions designation processes. Hordes of volunteers from around the world are scouring social media and the wider internet for information to tally Russia's losses, outline its shortfalls, combat its disinformation, and collate conflict news into easy-to-follow updates on the military situation.[14]

These contributions have boosted Ukraine's capability not only to fight in real time, but also to broadcast its messages and rally the world to support its aims. The ubiquity of sensors and recording devices has turned every individual into a potential source of information,[15] making some Russian propaganda that is reliant on fabrication difficult to sustain.[16] Finally, public relations services donated by Western firms have served as a way for Ukraine to influence the perceptions of enemy, allied, and neutral actors[17]—all without needing to expend scarce resources on expensive foreign consultants.

Ukraine's War Effort Reflects the Democratization of Intelligence

These new combat dynamics in Ukraine reflect the democratization of intelligence—a phenomenon whereby the increased availability of data and technology is enabling nonstate actors to participate in the production and dissemination of intelligence.[18] For most of the Cold War, sophisticated intelligence technology and tradecraft were the exclusive preserve of the world's top-tier intelligence agencies. But during the course of the past few decades, the proliferation of sensor technology, open data, and powerful algorithms has given nonstate organizations a unique ability to contribute across the continuum of intelligence operations. These "intelligence auxiliaries" are changing the intelligence landscape across a wide variety of mission sets. Ukraine is only one example: before that conflict, intelligence auxiliaries were monitoring Chinese missile proliferation,[19] tracking down the perpetrators of atrocity crimes in Cameroon,[20] tracing the assets of malign oligarchs worldwide,[21] and detecting GPS spoofing in Russia.[22] Famously, the investigative journalism group Bellingcat has unmasked Russian spies with regularity through the effective use of open-source and leaked data.[23]

Intelligence auxiliaries are changing the game. States and their agents are no longer the only actors in the production, analysis, and dissemination of intelligence. Nor are policymakers the only individuals toward whom intelligence production is directed. Instead, collection, production, and dissemination are becoming more matrixed, with the intelligence trade plied by individuals, nonprofits, and private corporations alongside traditional state actors. Rather than a set of staid bureaucracies driven by repeatable, well-known processes, the future of intelligence is that of a boisterous and unruly bazaar of data, tradecraft, capability, and insight.

Navigating this emerging marketplace of new capabilities and players will require engagement from states that are used to controlling the intelligence production process end to end. Ukraine's government deserves credit for skillfully integrating nonstate intelligence work and

volunteer energy into its overall war effort, but the course of the war has revealed several important questions about the future of intelligence in conflict environments, and about how states can effectively cooperate with nonstate actors. This *Research Short* does not seek to answer these questions—just to pose some of them.

The democratization of intelligence has empowered all, but it has empowered some more than others. The explosion of open-source information has empowered individuals and small organizations in ways that are rightly celebrated. Among nonstate intelligence actors, however, large private sector organizations endowed with significant financial and analytical resources have largely emerged as the main outside contributors to Ukraine's defense. The satellites that tracked the Russian buildup and have provided persistent targeting and data link,[24] as well as the AI technology deployed to track Russian communications,[25] are the products of well-funded, large organizations—not plucky individuals. Prominent data and analytical tool providers, such as private satellite companies,[26] are at the frontlines, traveling to Ukraine to engage its leaders.[27] The democratization of intelligence may mean that collection power could be more evenly distributed than it was during the era of state exclusivity, but it is still disproportionately concentrated in the hands of larger firms that have invested significant resources in the production of data and analytical tooling.

Ukraine has brought together significant capability through intelligence auxiliaries, but it has not created a unified command authority. Ukraine's government has been able to leverage non-Ukrainian groups independently seeking to contribute to Kiev's defense.[28] Whether through launching international volunteer battalions,[29] formal contracting,[30] soliciting grassroots donations,[31] combating cyberattacks,[32] or hacking and leaking information on the adversary for all and sundry to use,[33] the Ukrainian state has been able to draw on a wide range of capabilities, and ways of working, to accomplish its mission.[34]

But relying on outside groups comes with drawbacks. Without coordination, the international and patchwork nature of Ukraine's nonstate intelligence effort can complicate the conflict. For instance, commentators have noted how the performance of intelligence missions by non-uniformed, noncitizen personnel uncoordinated with the government in Ukraine complicates the application of the international laws of war.[35] Concerns about adversarial targeting of nonstate auxiliary capabilities are no longer hypothetical. Already, Russia has suggested that SpaceX's Starlink satellites might become "legitimate targets" because of their aid to the Ukrainian state;[36] might other nonstate actors conducting information gathering become seemingly valid targets? What about nonstate individuals navigating or repairing key military equipment in third countries? Or individuals based abroad using only publicly available information and their own data science skills to contribute to Ukraine's defense? If such actors are voluntarily participating in the conflict, are there any grounds for such actors to be legitimately targeted by lethal or nonlethal capabilities?

Variances in organizational form, capability, and activity among intelligence auxiliaries suggest the value of a flexible, adaptable command structure to coordinate activity. Although some intelligence auxiliaries interface closely with the formal structures of the

Ukrainian state (and its Western allies),[37] many simply take their own initiative and the tools at their disposal to support the overall mission as they perceive it. Some groups are clearly intertwined with Ukrainian military commanders,[38] while others, including many hacktivists, are managed through unofficial social media channels.[39] No central coordinating authority oversees it all; instead, command and control is replaced in many cases by loose affiliation or opportunistic enlistment by entrepreneurial policymakers on the scene.[40]

Without a unifying structure or doctrine, nonstate intelligence actors can operate much more nimbly, but they also risk polluting the information pool with unreliable information. The very techniques used by OSINT researchers have been mimicked by Russia to confuse facts on the ground,[41] and there is a real risk that, without coordination, nonstate intelligence actors may inadvertently spread disinformation, rather than debunking it. This can have deadly consequences on the battlefield, especially in situations where there is not enough time to carefully weigh and assess incoming information.

An Intelligence Partnership Holds Opportunities and Challenges

The war in Ukraine shows how an innovative strategy can bring together intelligence auxiliaries into an organization that is more than the sum of its parts. Such an "intelligence militia"—akin to the colonial militias that supported the Continental Army in our Revolutionary War—has become a material factor in Kiev's fight against the Russian invasion; however, it has emerged ad hoc, without conscious attention to maximizing the benefits and attenuating some of the risks outlined above.

Today, the United States and its allies have an opportunity to develop a structured and strategic framework—a policy roadmap—for working effectively with nonstate intelligence auxiliaries and preparing for the challenges that such collaboration could pose. This opportunity is closely tied to the longer running need to better integrate open-source data into the intelligence enterprise—but it goes a step further. Although some members of the U.S. Intelligence Community (IC) recognize the importance of acquiring and leveraging both open-source and commercial information,[42, 43] such data are typically viewed as additional fodder for the IC's own analysts, not as part of a framework to align nonstate actors to U.S. policy goals. Nonstate actors, although important to conflict dynamics around the world, are typically left out of the planning picture. This leaves significant capability unaccounted for in policymakers' planning.

But intelligence auxiliaries are not going away, and in future conflicts, nonstate actors will continue to collect, analyze, and disseminate information in ways that affect operations at the tactical and strategic levels—and not always to the benefit of the United States. Misguided, enthusiastic amateurs can cause as much harm as enemy actors when they are not integrated into ongoing operations. Rather than ignore these groups, the United States has an opportunity to create structures to bring them effectively into the fight, maximizing the benefits of their activity while minimizing the costs. (Please see the Appendix for discussion of specific opportunities and challenges to be considered in integrating an intelligence militia.)

Looking Ahead: Implications for the IC

Nonstate intelligence is here to stay. But the rise of intelligence auxiliaries does not presage the end of state capability, the demise of secrets, or the transformation of all intelligence into OSINT. Instead, it points to a future where a more effective form of public-private partnership between state and nonstate intelligence actors is possible.

For the Intelligence Community, the time is now to craft a long-term strategy for what these public-private intelligence partnerships should look like. As a first step, the IC should map the nonstate analytical ecosystem—identifying the actors, data sources, funding streams, and incentives behind the production of intelligence outside of state frameworks. As part of this effort, the IC should consider foundational questions for the design of this ecosystem, including but not limited to the following:

- **Analytical standards underlying collaboration with friendly intelligence auxiliaries.** These standards would include not only how state actors can properly assess the credibility of information derived from nonstate sources, but also how the IC can encourage interoperability between separate nonstate actors when doing so is in the interest of the state (as it is, for instance, with NGO reporting on suspicious activities to financial institutions). Analytical standard development should take advantage of burgeoning efforts within both the U.S. and foreign nonstate analytical communities to develop standards for OSINT collection and analysis.
- **Securing the U.S. and allied ICs from the activities of adversary intelligence auxiliaries, especially when doing so may run counter to traditional stances around civil liberties.** An increased level of collaboration with nonstate intelligence auxiliaries is likely to increase the attack surface available to foreign adversary organizations. Before engaging headlong with a wide variety of often inexperienced organizations, the IC should develop simple, external-facing, and secure means of collaboration to ensure any risk is effectively limited.
- **Ensuring a robust funding ecosystem for the technologies and actors that empower nonstate intelligence.** Intelligence auxiliaries may not use classified information, but this does not mean they do not need to purchase exquisite capabilities of their own—including satellite imaging or data analysis capabilities. A review of the funding ecosystem would include examining not only the role of government support through grants and contracts, but also the degree to which private and venture funding is promoting the development of the tooling and analytical capabilities needed for a robust nonstate analytical ecosystem.
- **Curating the information environment to maximize the available pool of accurate, relevant, and reliable publicly available information (PAI).** Nonstate intelligence relies on sifting through vast pools of PAI for signal; the United States and its allies can help create more signal by encouraging foreign jurisdictions to increase the availability of data sources, such as open corporate registries or trade data streams, that

are core to the work of intelligence auxiliaries. At the same time, the United States should examine how a lack of regulation around data brokers may be unhelpfully contributing to the activities of adversary state and nonstate intelligence actors.

- **Finally, addressing a range of legal questions surrounding the activity of intelligence auxiliaries.** These questions would include addressing the permissibility of directly tasking nonstate actors and the degree to which nonstate intelligence actors must comply with laws restricting the IC's activity, as well as questions surrounding the applicability of the law of armed conflict to intelligence auxiliaries engaged in battlefield support tasks. Leaving these questions open to case-by-case interpretation—especially in armed conflict—increases the risk that intelligence auxiliaries may act in a way that violates important legal norms and standards to which the professional IC adheres.

The United States can go in many directions in its future interactions with nonstate intelligence auxiliaries, but it does not have the option to simply ignore them. For future conflicts where state and nonstate actors can both bring capability to the table, any strategy is better than no strategy. The U.S. IC has a unique opportunity to work on that strategy now, ahead of the next conflict.

Thomas Ewing has led teams using open-source information to support tactical and operational decisionmaking in U.S. and allied governments. He is a graduate of the Harvard Law School and an officer in the U.S. Naval Reserve. This paper reflects his personal views and not those of any institution with which he is affiliated.

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

Appendix: The Opportunities and Challenges of an Intelligence Militia

Opportunities

A long-term strategy for leveraging nonstate analytical expertise ideally could introduce enough structure to guide and incentivize intelligence auxiliaries, while maintaining enough flexibility to adapt to future technological advances in open-source intelligence. Because intelligence auxiliaries have few clear points of contact with the government, establishing a network of dedicated offices responsible for outside liaison within appropriate elements of the IC—at the ODNI, agency, or COCOM level—could facilitate information exchange and loose coordination between state and nonstate actors:

- **Liaising with the nonstate analytical community.** Liaison offices could serve as the main point of contact between the IC and intelligence auxiliaries, fielding inquiries, communicating national goals, understanding the needs of the analytical community, combating misinformation, and working to coordinate the actions of intelligence auxiliaries with state aims. This office's remit would be not only national, but also international, reflecting the international nature of the intelligence militia. Templates for this type of organization already exist: the stakeholder engagement office of Canada's intelligence services[44] and the 2020 National Defense Authorization Act's proposed Social Media Data and Threat Analysis Center[45] are two prominent examples of government seeking to bring nonstate actors into important national security arenas.
- **Orchestrating the diverse capabilities of intelligence auxiliaries.** Such a liaison office could target specific intelligence auxiliaries who bring complementary and non-duplicative capabilities to the effort and ensure that auxiliaries and IC are working as a team and not at cross purposes. The office could also serve as a market maker, introducing intelligence auxiliaries with valuable software, data, or consulting services to appropriate customers in the U.S. Government and coordinating a healthy long-term market for intelligence services.
- **Devising agile, mission-centered contractual frameworks that provide a quick "on ramp" for intelligence auxiliaries.** The war in Ukraine has allowed corporate intelligence auxiliaries to demonstrate their technology in a mission-oriented environment, but this has happened largely spontaneously and through individual corporate initiative. Although the outpouring of support for Ukraine has been significant, a future conflict may not see as many corporate intelligence auxiliaries rallying to the flag—meaning that the United States and its allies would need to deploy other incentives, including financial, to attract participants. By providing agile contracting solutions, a liaison office could connect commercial analytical capabilities with mission requirements, helping intelligence auxiliaries field capabilities faster.
- **Curating the information environment to give intelligence auxiliaries access to high-quality data and analytical tools.** Intelligence auxiliaries make excellent use of

public data and technology, but the information environment is constantly under threat from state restriction and misinformation. The IC has a vested interest in making sure that nonstate OSINT actors have access to reliable, quality information from multiple sources and from around the world; the United States and its allies could define an open data architecture that is transparent and designed to make data maximally accessible to intelligence auxiliaries. The United States could also lead the way in evaluating its own holdings for increased transparency,[46] while encouraging others to adhere to world-class standards for open data.

Challenges

Creating a long-term structure for public-private intelligence partnerships (i.e., integrating an intelligence militia) would certainly have its challenges—indeed, the conflict in Ukraine has revealed several problems that come from greater nonstate intelligence activity. But the United States and its allies have a window to think through challenges ahead of time and to ensure that, the next time nonstate actors involve themselves in conflict, there is a more rigorous framework for assessing tradeoffs:

- **Using an intelligence militia will challenge U.S. domestic intelligence law.** U.S. domestic intelligence law was shaped, following painful experiences with spying on Americans and bulk collection, to include a core distinction between collecting on U.S. citizens and noncitizens. More generally, intelligence as practiced in democratic societies has evolved to include restrictions on what intelligence agencies can and cannot collect. The framework of an intelligence militia—if not formally bound by contract with the U.S. Government that includes accountability to U.S. law—risks creating a situation where intelligence agencies can simply get around democratic norms and laws by encouraging private actors to engage in collection on their behalf. Ensuring that intelligence auxiliaries are not used to sidestep valuable privacy and civil liberties protections would require a carefully balanced framework for collaboration.
- **An intelligence militia poses a challenge to the international laws of war—and the laws of espionage.** International Humanitarian Law depends on distinguishing between combatants and noncombatants, affording the latter protection from targeting. Spies, though less protected than armed combatants, are still given some protections by international law.[47] But in a world where technology enables civilians in any part of the world to participate in intelligence operations on a voluntary, part-time basis, these distinctions can become difficult to observe.[48] The United States and its allies cannot necessarily control how intelligence auxiliaries are treated by adversaries, but they can help establish explicit norms and ways of working that will at least provide guidance to individuals and organizations whose employees may find themselves accused of espionage by unfriendly regimes.
- **Intelligence auxiliaries can radically change the escalation dynamics of a conflict.** Intelligence auxiliaries can cause a conflict to escalate in intensity—sometimes

intentionally against the design of state actors engaged in the conflict. Intelligence auxiliaries may seek to shape the conflict according to their own aims, whether through independent targeting and strikes, information operations, or some other activity that affects events on the ground in ways unintended by state actors. Such efforts may cause the other coalition to respond in kind, prolonging the conflict and making de-escalation difficult, even if de-escalation is in the interests of both combating coalitions. Avoiding harmful escalation spirals—possibly through clear "rules of the road" with accountability, or even a central command authority—should be a priority of any framework for relations between state actors and intelligence auxiliaries.

- **Relying on intelligence auxiliaries may increase the attack surface of our own intelligence efforts.** An intelligence militia might provide more areas for adversaries to deploy human, cyber, or other intelligence tools to discover plans and sow discord. Ensuring that trusted intelligence auxiliaries have been taught—and adhere to—high standards of cyber and personnel hygiene could lower the risk of espionage by unfriendly powers.

Endnotes

1 Sandra Erwin, "As Russia Prepared To Invade, U.S. Opened Commercial Imagery Pipeline to Ukraine," *SpaceNews*, April 6, 2022, https://spacenews.com/as-russia-prepared-to-invade-u-s-government-and-satellite-imagery-suppliers-teamed-up-to-help-ukraine/.

2 Christopher Miller, Mark Scott, and Bryan Bender, "UkraineX: How Elon Musk's Space Satellites Changed the War on the Ground," *Politico*, June 8, 2022, https://www.politico.eu/article/elon-musk-ukraine-starlink/.

3 Alia Shoaib, "Inside the Elite Ukrainian Drone Unit Founded by Volunteer IT Experts: 'We Are all Soldiers Now.'" *Business Insider*, April 9, 2022, https://www-businessinsider-com.cdn.ampproject.org/c/s/www.businessinsider.com/inside-the-elite-ukrainian-drone-unit-volunteer-it-experts-2022-4?amp.

4 Matt Burgess, "Their Photos Were Posted Online. Then They Were Bombed," *Wired*, August 26, 2022, https://www.wired.com/story/wagner-group-osint-russia-ukraine/.

5 Amra Dorjbayar et al., "Killer Coordinates: How a Russian Missile Hit Kyiv With the Help of Online Sleuths," Centre for Information Resilience, June 15, 2022, https://www.info-res.org/post/killer-coordinates-how-a-russian-missile-hit-kyiv-with-the-help-of-online-sleuths.

6 "CRDF Global Becomes Platform for Cyber Defense Assistance Collaborative (CDAC) for Ukraine, Receives Grant from Craig Newmark Philanthropies," CRDF Global (press announcement), November 14, 2022, https://www.crdfglobal.org/news/crdf-global-becomes-platform-for-cyber-defense-assistance-collaborative-cdac-for-ukraine-receives-grant-from-craig-newmark-philanthropies/;.

7 Dina Temple-Raston, "41. Rounding Up a Cyber Posse for Ukraine," Click Here (podcast), November 15, 2022, https://open.spotify.com/episode/58ARqJc1kLP7PyvVyiaLn5?si=i5PmsocbQamY5kKYomNyOQ&nd=1.

8 Will Knight, "As Russia Plots Its Next Move, an AI Listens to the Chatter," *Wired*, April 4, 2022, https://www-wired-com.cdn.ampproject.org/c/s/www.wired.com/story/russia-ukraine-war-ai-surveillance/amp.

9 Cory Doctorow, "About Those Kill-switched Ukrainian Tractors," *Medium*, May 8, 2022, https://doctorow.medium.com/about-those-kill-switched-ukrainian-tractors-bc93f471b9c8.

10 Laura Italiano, "Ukraine is Using Facial Recognition To ID Dead Russian Soldiers and send Photos of Corpses Home to Their Moms: report," *Business Insider*, April 15, 2022, https://www.businessinsider.com/ukraine-sending-photos-of-dead-russian-soldiers-home-moms-2022-4?r=US&IR=T.

11 Mehul Srivastava, "Ukraine's Hackers: an Ex-spook, a Starlink and 'Owning' Russia," *Financial Times*, September 4, 2022, https://www.ft.com/content/f4d25ba0-545f-4fad-9d91-5564b4a31d77.

12 "New Site Allows Users To Crank Call Russian Bureaucrats To Protest War in Ukraine," Gizmodo, May 18, 2022, https://gizmodo.com/waste-russian-time-prank-call-ukraine-war-protest-putin-1848942119.

13 Human Rights First, "NGOs Identify Human Rights Abusers, Corrupt Actors for Sanctions Under U.S. Bill," Press Release, September 13, 2017, https://www.humanrightsfirst.org/press-release/ngos-identify-human-rights-abusers-corrupt-actors-sanctions-under-us-bill.

14 Ross Burley, "Disinformation & Denial: Russia's Attempts To Discredit Open Source Evidence of Bucha," Centre for Information Resilience, April 13, 2022, https://www.info-res.org/post/disinformation-denial-russia-s-attempts-to-discredit-open-source-evidence-of-bucha.

15 Billy Perrigo, "How Open Source Intelligence Became the World's Window Into the Ukraine Invasion," *Time*, February 24, 2022, https://time.com/6150884/ukraine-russia-attack-open-source-intelligence/.

16 Amanda Seitz and Arijeta Lajka, "Amid Horror in Bucha, Russia Relies on Propaganda and Disinformation," PBS News Hour, April 6, 2022, https://www.pbs.org/newshour/world/amid-horror-in-bucha-russia-relies-on-propaganda-and-disinformation.

17 "Ukraine's Information War Is Winning Hearts and Minds in the West," *The Conversation*, May 12, 2022, https://theconversation.com/ukraines-information-war-is-winning-hearts-and-minds-in-the-west-181892.

18 Thomas Ewing, "The Real Power of Intelligence 'Auxiliaries,'" *The Cipher Brief*, February 21, 2022, https://www.thecipherbrief.com/the-real-power-of-intelligence-auxiliaries.

19 Matt Korda and Hans Kristensen, "China Is Building a Second Nuclear Missile Silo Field," Federation of American Scientists, July 26, 2021, https://fas.org/blogs/security/2021/07/china-is-building-a-second-nuclear-missile-silo-field/.

20 "Cameroon: Anatomy of a Killing - BBC Africa Eye documentary," *BBC News*, September 23, 2018, https://www.youtube.com/watch?v=XbnLkc6r3yc.

21 Tom Stocks, "10 Tips for Tracking Russian-Owned Assets," Global Investigative Journalism Network, March 17, 2022, https://gijn.org/2022/03/17/10-tips-for-tracking-russian-owned-assets/.
22 "Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria," Center for Advanced Defense Studies, 2019, https://www.c4reports.org/aboveusonlystars.
23 Shaun Walker, "Socialite Who Charmed NATO Staff in Naples Was Russian Spy, Say Investigators," *The Guardian*, August 26, 2022, https://www.theguardian.com/world/2022/aug/26/socialite-who-charmed-nato-staff-in-naples-was-russian-spy-say-investigators.
24 Mariel Borowitz, "War in Ukraine Highlights Importance of Private Satellite Companies," *Astronomy*, August 16, 2022, https://astronomy.com/news/2022/08/war-in-ukraine-highlights-importance-of-private-satellite-companies.
25 Will Knight, "As Russia Plots Its Next Move, an AI Listens to the Chatter.
26 Sandra Erwin, "Maxar Eager To Launch New Satellites Amid Soaring Demand for Imagery Over Ukraine," *SpaceNews*, April 11, 2022, https://spacenews.com/maxar-eager-to-launch-new-satellites-amid-soaring-demand-for-imagery-over-ukraine/#:~:text=3D%20mapping%20of%20Ukraine,after%20representations%20of%20the%20damage.
27 Olafimihin Oshin, "Palantir CEO Travels to Ukraine for Zelensky Meeting," *The Hill*, June 6, 2022, https://thehill.com/policy/technology/3513256-palantir-ceo-travels-to-ukraine-for-zelensky-meeting/.
28 "Star Maker: Ukraine's Use of Private Sector Satellite Services," *Key.Aero*, June 13, 2022, https://www.key.aero/article/star-maker-ukraines-use-private-sector-satellite-services.
29 "Russia Invaded Ukraine: Enlist to the International Legion of Defence of Ukraine, International Legion/Defence of Ukraine, Fightforua, accessed on August 26, 2022, https://fightforua.org/.
30 ICEYE, "ICEYE Signs Contract To Provide Government of Ukraine With Access to Its SAR Satellite Constellation," Press Release, August 18, 2022, https://www.iceye.com/press/press-releases/iceye-signs-contract-to-provide-government-of-ukraine-with-access-to-its-sar-satellite-constellation.
31 Amitoj Singh, "Ukraine Bought Weapons, Drones With Crypto Donations," CoinDesk, August 17, 2022, https://www.coindesk.com/policy/2022/08/17/Ukraine-bought-weapons-drones-with-crypto-donations/.
32 David Ignatius, "Opinion: How Russia's Vaunted Cyber Capabilities Were Frustrated in Ukraine," *Washington Post*, June 21, 2022, https://www.washingtonpost.com/opinions/2022/06/21/russia-ukraine-cyberwar-intelligence-agencies-tech-companies/.
33 Collier, Kevin.,"Hackers Flood Internet With What They Say Are Russian Companies' Files," *NBC News*, April 5, 2022, https://www.nbcnews.com/tech/security/hackers-flood-internet-say-are-russian-companies-files-rcna21853.
34 Ewing, "The Real Power of Intelligence 'Auxiliaries.'"
35 Kate Kilgore, "405. Democratized Intelligence," Mad Scientist Laboratory, June 30, 2022, https://madsciblog.tradoc. army.mil/405-democratized-intelligence/.
36 Tara Brown, "Can Starlink Satellites Be Lawfully Targeted?" Lieber Institute (West Point) *Articles of War*, August 5, 2022, https://lieber.westpoint.edu/can-starlink-satellites-be-lawfully-targeted/#:~:text=Russia%20has%20the%20capability%20to,could%20be%20used%20to%20target.
37 Ignatius, "Opinion: How Russia's Vaunted Cyber Capabilities Were Frustrated in Ukraine."
38 Burgess, "Their Photos Were Posted Online. Then They Were Bombed."
39 Hannah Murphy, "Ukraine War Sparks Revival of Hacktivism," *Financial Times*, March 4, 2022, https://www.ft.com/content/9ea0dccf-8983-4740-8e8d-82c0213512d4.
40 Ewing, "The Real Power of Intelligence 'Auxiliaries.'"
41 Justin Ling, "Russia Is Mimicking Open-Source Intelligence Methods To Discredit Bucha Atrocities," *Foreign Policy*, April 12, 2022, https://foreignpolicy.com/2022/04/12/russia-open-source-intelligence-bucha-atrocities/.
42 Aki Peritz, "Building an Open-Source Intelligence Buyer's Club," *War on the Rocks*, October 20, 2022, https://warontherocks.com/2022/10/building-an-open-source-intelligence-buyers-club/;
43 National Geospatial Intelligence Agency, "Commercial GEOINT Strategy," Resources, accessed August 26, 2022, https://www.nga.mil/resources/Commercial_GEOINT_Strategy.html.
44 Government of Canada Canadian Security Intelligence Service "Academic Outreach and Stakeholder Engagement,", accessed September 24, 2022, https://www.canada.ca/en/security-intelligence-service/corporate/academic-outreach.html.

45 Steven Bradley, "Securing the United States From Online Disinformation – A Whole-of-Society Approach," Carnegie Endowment for International Peace, August 24, 2020, https://carnegieendowment.org/2020/08/24/securing-united-states-from-online-disinformation-whole-of-society-approach-pub-82549.

46 Garrett Berntsen and Ryan Fedasiuk, "To Defeat Autocracy, Weaponize Transparency," *War on the Rocks*, August 23, 2022, https://warontherocks.com/2022/08/to-defeat-autocracy-weaponize-transparency/.

47 International Committee of the Red Cross, "Practice Relating to Rule 107. Spies. Section B. Status of Spies," International Humanitarian Law (IHL) database, accessed August 26, 2022, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule107_sectionb.

48 Lukasz Olejnik, "Smartphones Blur the Line Between Civilian and Combatant," *Wired*, June 6, 2022, https://www.wired.com/story/smartphones-ukraine-civilian-combatant/.