MITRE | Intelligence After Next

2025 PRESIDENTIAL TRANSITION SPECIAL EDITION

RADICAL TRANSPARENCY: EXPANDING PARTNERSHIPS WITH COMMERCIAL INTELLIGENCE SHARING

by Christian Neubauer

With the recent release of the 2023 National Intelligence Strategy (NIS), MITRE is publishing a special series of Intelligence After Next papers aligned to each of the six NIS goals the Intelligence Community will pursue over the next four years in support of U.S. national security strategies and priorities. Each paper will focus on an aspect of an NIS goal and offer a road map for success. This paper is aligned to Goal 4: Diversify, Expand, and Strengthen Partnerships.

Transparency as an Intelligence Strategy

The first few years of this decade have been a resounding success for transparency in U.S. intelligence. While few outside of the Intelligence Community (IC) may have taken notice of the 2015 release of a Director of National Intelligence implementation plan on intelligence transparency,[1] the American public and our partner nations have recognized the IC's practical efforts to share intelligence in recent years. These include public exposure of Russia's buildup to the invasion of Ukraine, release of geospatial data showing China's militarization of the South China Sea, and the unprecedented intelligence sharing efforts the United States is pursuing with nations well beyond our traditional Five Eyes (FVEY) partners.[2] The IC has even led the way in thinking on generational challenges regarding the use of technology for governance, such as ethics in the use of artificial intelligence. As a result, the IC finds itself in a hard-earned position of trust within the public consciousness, scoring highly on questions of trust[3] despite widespread global distrust in public institutions.[4]

Authoritarian governments, with increasingly complex intelligence capabilities of their own, seek to erode that trust with disinformation and malign influence. In this environment, transparency is a differentiated value the IC can build on with partner nations and the global citizenry. We must arm our partners with the tools they need to maintain free and sovereign societies while at the same time growing the alliances and partnerships that form the crux of our "enduring strength."[5] Commercial intelligence can be a tool toward this end, helping the United States build partner intelligence capacity to secure their borders, maintain election integrity free of foreign influence, and understand and cope with food and water security issues. The United States should share commercial data, tradecraft, and our ethical intelligence foundation with partners to inoculate them against those countries that would exploit others to their own advantage.

Transparency Lessons from the Russian Invasion of Ukraine

Despite the challenges of gaining broad acceptance of the U.S. government narrative that Russia intended to invade Ukraine prior to 24 February 2022, it was clear immediately after the invasion that U.S. intelligence on the topic was detailed, voluminous, and convincing. The United States had what amounted to the detailed plan of invasion of Ukraine before it happened.[6] Because the United States chose to pursue intelligence transparency, as the Director General of the Estonian Foreign Intelligence Service said, "everybody was on the same sheet of music when the war started."[7]

The lessons for the United States were clear:

- Sharing with partners has an incredible trust-building effect even if it fails to deter the adversary.
- Observable data is significantly more valuable to our partners than analytic judgments without supporting data.

This sharing effort built a level of trust that clear intelligence failures during the leadup to the invasion of Iraq in 2003 shattered and that decades of vague U.S. statements without the support of raw data had failed to rebuild. This expanded sharing in the case of the Russian invasion of Ukraine has led to similar disclosures:

- The Defense Intelligence Agency (DIA) released information on Iranian drone shipments to Russia.[8]

- The National Security Agency (NSA) and U.S. Cyber Command have begun disclosure of previously classified adversary cyber activity to the public.[9]
- U.S. Africa Command (USAFRICOM) has released intelligence on Russian and Wagner Group activities in the ongoing civil war in Libya.[10, 11]
- The National Geospatial-Intelligence Agency (NGA) has established a website, Tearline.mil, dedicated to publicly sharing intelligence.

These sharing efforts are paying dividends in our relationships with partners.

Risk Aversion Hampers Our Success

Despite these successes, there is still tension within the IC about how much to share with partners and whether we might inadvertently expose “sources and methods” to our adversaries. As documented in a *Washington Post* deep dive on the leadup to the Ukraine crisis, senior officials in the IC were still reluctant to share information on how we knew what we knew,[12] and without that level of insight, it was hard for other nations to trust our judgment. This is not a new concern, of course—volumes have been written on the tradeoffs of publicly sharing classified intelligence that date from U-2 imagery released during the Cuban Missile Crisis[13] to the Cold War.[14] The overriding concern in the IC remains that sharing intelligence might lead our adversaries to figure out how we figured it out and turn off whatever access we had to that insight.[15]

To overcome this challenge, the Department of Defense (DoD) and the IC have traditionally relied on classified intelligence sharing systems that allow the U.S. and specific allied organizations to trade digital intelligence products. These systems are protected by robust rules and regulations to keep them secure. Unfortunately, the systems are also cumbersome, expensive to install, onerous to maintain, and work for only a small subset of our allies. For those partners without the internal infrastructure and policy in place to support U.S.-equivalent classification markings or who lack an established relationship with the U.S. to share intelligence, these systems are difficult or impossible to use.

Even for partner nations with relatively advanced intelligence communities—like the Five Eyes partners with which we have decades-old, well-defined sharing processes—the complexity of policy and system accesses still causes significant hurdles to sharing.[16] For less robust or well-funded intelligence organizations—like those of nontraditional partners that we rely on in Ukraine and will rely on for any conflict with China—the United States can establish a specialized classified infrastructure and give the partner nation some allocation of computer equipment to connect to that infrastructure. Because we are essentially extending trust to another nation that they will manage and protect U.S. secrets, we are very cagey about who in that partner nation can have access. We may give systems to a specific group or groups within a partner Intelligence Community, or maybe only to certain individuals. However, as the 2004 9/11 Commission Report pointed out, this sort of siloed intelligence sharing is a recipe for disaster.[17]

At the same time, DoD is spending millions on Mission Partner Environments (MPE)[18] that are essentially classified systems designed and built by the United States and given to partners as sharing solutions. MPE is advertised as a secure solution to sharing, built on all the currently popular techniques for security like Zero Trust, Edge Cloud, and Data Centric Security. But MPEs do not address the underlying trust issue. We do not trust partner nations enough to give them the unfettered access to our raw intelligence that they need to understand, decide, and act.

Commercial Intelligence Offers a Way Forward

There is an intriguing way out of this conundrum for the IC. In recent years, the IC has taken steps to share intelligence with partners in unclassified venues, such as the NGA’s previously mentioned Tearline.mil, the Protected Internet Exchange (PiX), and U.S. Southern Command’s Enhanced Domain Awareness (EDA). These efforts focus on expanding access beyond FVEY partners, and beyond even government entities to nongovernmental organizations, citizen groups, commercial organizations, and others that can create positive impact aligned to U.S. and partner interests. These platforms take heavy advantage of commercial intelligence.

Commercial intelligence capabilities are beginning to rival those of even the best funded governmental intelligence organizations.

- Commercial space constellations offer multiple modalities for sensing and observing the earth, including tracking illegal fishing fleets with synthetic aperture radar (SAR)[19] and identifying jammers via radiofrequency emissions.[20]
- Vendors track supply chains, construction activities, and crop growth with smartphone applications.[21, 22]
- Commercial intelligence companies look for bot armies promoting malign influence, and they monitor election interference campaigns through social media.[23]

These capabilities provide commoditized intelligence previously the unique domain of well-funded national intelligence communities. Today, they can help the United States expand the capabilities of our partners and allies without compromising sources and methods.

As we have seen in Mali, Afghanistan, Sudan, and elsewhere, U.S. foreign aid in the form of weaponry and military training can easily be used against U.S. interests or, even more tragically, against the civilian populace. Headlines like "Coup Plotters in Mali Were Trained by U.S. Military" do not exactly engender trust.[24] Intelligence capacity building offers the same challenges. Sell a country better face recognition technology—like the Chinese are doing as part of their Safe City initiative—and they may well identify and arrest political dissenters using that technology. For example, cell phone intercept technology sold to Saudi Arabia and the United Arab Emirates (UAE) may be used to monitor the civilian population.[25]

Rather than jumping into the whirlpool of determining how to regularly and repeatedly declassify intelligence to share with non-FVEY partners or building another unique walled intelligence sharing system, the United States should enable partners to see what we see through commercial intelligence.

There are opportunities, however, to help a country grow its intelligence capabilities in ways that promote democracy and sovereignty against foreign influence. These include:

- Sensing and analysis to monitor the earth and atmosphere to create resilient food and water systems.
- Monitoring information campaigns intended to disrupt elections.
- Protecting critical infrastructure from cyber-attacks by state and non-state actors.
- Tracking natural resources including fish, timber, and minerals and attempts at illegal exploitation by poachers, traffickers, and smugglers.

By sharing commercial intelligence capabilities with our allies, we promote a level playing field for democratized intelligence. This will build trust and strengthen partnerships while also serving as a force multiplier for our own IC—expanding our sensor networks; inoculating our partners against foreign malign activity; and growing a cadre of intelligence professionals in partner nations trained on the value of ethics, analytic standards, apolitical reporting, and transparency.

Building Intelligence Capacity with Partners

The U.S. government has multiple programs in place to build partner capacity. Title 10 sections 331, 332, and 333,[26] for example, authorize the Secretary of Defense to train and equip foreign countries. The United States uses these mechanisms to help partners improve their cyber defensive capabilities, making them more effective at detecting and countering cyber-attacks. These efforts help pull other countries into a shared United Nations framework for operating within the "rules of the road" on cyberspace.[27] This is an obvious net good for the United States and the world. The United States needs a similar program designed to improve partner intelligence capacity. The impact of this program would be a similar net good where partners are better able to "seek the truth; speak truth to power; and obtain, analyze, and provide intelligence objectively."[28]

Rather than jumping into the whirlpool of determining how to regularly and repeatedly declassify intelligence to share with non-FVEY partners or building yet another unique walled intelligence sharing system, the United States should enable partners to see what we see through commercial intelligence. Commercial geospatial intelligence, electronic intelligence (ELINT), open-source intelligence, and other services can provide significant capabilities to warn of impending attack in eastern Europe; detect malign influence campaigns in Africa; or monitor illegal Chinese fishing fleets in South America, Asia, and Oceania. The United States can also provide the critical missing pieces in the commercial intelligence equation: analytic tradecraft and the foundational ethical underpinning that drive our processes and policies. We can achieve this by acting in several ways, including:

- Significantly expanding PiX, EDA, Tearline.mil, and similar efforts with both additional resources and new partners. DIA, NGA, NSA, and other analytic organizations should invest in the commercial data services and the analysts needed to feed these platforms, reprioritizing resources from classified efforts where necessary to achieve this critical National Intelligence Strategy goal. Wherever possible, the United States should broaden the scope of these systems to include nongovernmental organizations, industry, academia, and other public institutions to avoid the trap of enabling governments to work against their own people.
- Working directly with key partners such as Poland, Finland, the Baltic States, Ghana, Nigeria, Kenya, Colombia, Peru, Chile, Argentina, Taiwan, the Philippines, and Vietnam to identify and close their intelligence capability gaps with commercial intelligence. This should include providing funding and licenses for data, training on analytic methods and ethics, prototypes against specific partner nation use cases, and other initiatives developed with the partner as part of a formal collaboration for capacity building—similar to the processes used for existing security cooperation initiatives.[29] These efforts should be folded into existing strategic partnerships and exercises with those nations to ensure they align to national strategy.

The Benefit of Truth on Our Side

This concept is predicated on the idea that we do, in fact, have the truth on our side; we believe in the continuity of the rules-based international order; and an alliance of like-minded nations benefiting from that international order will work in their own self-interest with us, if they have the tools and capabilities to do so. There is no guarantee the political goals of partner nations will not change over time in ways that are incompatible with U.S. interests. However, as with better cyber defense, better intelligence capabilities that protect a nation from attack, malign influence, and violations of sovereignty are innately good for global stability and security. The U.S. IC has the experience, expertise, and trust to work transparently with our partners to build a bulwark against malign influence and criminal activity.

References

1. Office of the Director of National Intelligence, Principles of Intelligence Transparency for the Intelligence Community, 2015. Available: https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic
2. Australia, Canada, New Zealand, the United Kingdom, and the United States.
3. The Chicago Council on Global Affairs, 2020 Public Attitudes on US Intelligence, 2021. Available: https://globalaffairs.org/research/public-opinion-survey/public-attitudes-us-intelligence-2020
4. Gallup, Confidence in Institutions, 2023. Available: https://news.gallup.com/poll/1597/confidence-institutions.aspx
5. Christopher Prawdzik, With NDS as a Guide, DOD Pursues Stronger Partnerships, 2023. Available: https://www.airandspaceforces.com/karlin-reiterates-integrated-defense-strategy-with-focus-on-chinese-and-russian-threats/
6. Shane Harris, Karen DeYoung, et al., Road to War: U.S. Struggled to Convince Allies, and Zelensky, of Risk of Invasion, 2023. Available: https://www.washingtonpost.com/national-security/interactive/2022/ukraine-road-to-war/
7. Julian Barnes and Adam Entous, How the U.S. Adopted a New Intelligence Playbook to Expose Russia's War Plans, 2023. Available: https://www.nytimes.com/2023/02/23/us/politics/intelligence-russia-us-ukraine-china.html
8. DIA, Iranian UAVs in Ukraine: A Visual Comparison, 2023. Available: https://www.dia.mil/Portals/110/DIA_Iranian_UAVs_in_Ukraine-A_Visual_Comparison.pdf
9. Mark Pomerleau, Intel disclosures Becoming "Instrument of Power" to "Throw Adversaries Off Their Game," 2022. Available: https://defensescoop.com/2022/04/20/intel-disclosures-becoming-instrument-of-power-to-throw-adversaries-off-their-game/
10. USAFRICOM, Russia and the Wagner Group Continue to Be Involved in Ground, Air Operations in Libya, 2020. Available: https://www.africom.mil/pressrelease/33034/russia-and-the-wagner-group-continue-to-be-in
11. USAFRICOM, Russia Deploys Military Fighter Aircraft to Libya, 2020. Available: https://www.africom.mil/pressrelease/32887/russia-deploys-military-fighter-aircraft-to-l
12. Shane Harris, Karen DeYoung, et al., Road to War: U.S. Struggled to Convince Allies, and Zelensky, of Risk of Invasion, 2023. Available: https://www.washingtonpost.com/national-security/interactive/2022/ukraine-road-to-war/
13. Adam Bejger, Photo Intelligence and the Cuban Missile Crisis, 2004. Available: https://digitalcommons.unf.edu/cgi/viewcontent.cgi?article=1077&context=ojii_volumes
14. James Walsh, The International Politics of Intelligence Sharing, 2010. Available: https://www.jstor.org/stable/10.7312/wals15410
15. Joshua Huminski, Russia, Ukraine, and the Future Use of Strategic Intelligence, 2023. Available: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_10-3/prism_10-3_8-25_Huminski.pdf?ver=7kbBfjYhi02aI4RjbWIkhA%3d%3d
16. For an in-depth account of the issues involved, see the Atlantic Council's excellent report on this challenge: Sean Corbett and James Danoy, Beyond NOFORN: Solutions for Increased Intelligence Sharing among Allies, 2022. Available: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-noforn-solutions-for-increased-intelligence-sharing-among-allies/
17. National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report, 2004. Available: https://govinfo.library.unt.edu/911/report/911Report.pdf
18. DoD Chief Information Officer, Mission Partner Environment Information Sharing Capability Implementation for the DoD, 2021. Available: https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/811001p.pdf

19. Satim, Fishing Secrets and SAR Technology, 2021. Available: https://www.satim.co/2022/09/15/fishing-secrets-and-sar-technology/
20. Janet Yurechko, Taking the Battle to Space: Detecting & Geolocating GPS Jamming Signals, 2021. Available: https://spire.com/blog/federal/detecting-geolocating-gps-jamming-signals/
21. Premise, Leading Multinational Consumer Goods Company Utilities Premise to Map First Mile Supply Chain, 2023. Available: https://www.premise.com/wp-content/uploads/2022/03/Case-Study-Palm-Fruit-Supply-Chain-Due-Diligence.pdf
22. Alexandra Wilson, Combining Satellite Data with Ground Observations in Partnership with Planet Federal, 2023. Available: https://www.premise.com/blog/combining-satellite-data-with-ground-observations-in-partnership-with-planet-federal/
23. Ben Dubow, Detecting and Countering Malign Influence Operations, 2022. Available: https://www.oodaloop.com/archive/2022/01/07/ben-dubow-on-detecting-and-countering-malign-influence-operations/
24. Robbie Gramer and Chloe Hadavas, Coup Plotters in Mali Were Trained by U.S. Military, 2020. Available: https://foreignpolicy.com/2020/08/21/mali-coup-trump-administration-counterterrorism-efforts-sahel-west-africa-us-training/
25. Joseph Cox, Data Shows How the UK Grants Licenses to Export Interception Tech, 2016. Available: https://www.vice.com/en/article/8q8vek/data-shows-how-the-uk-grants-licences-to-export-interception-tech-imsi-catchers
26. United States, Title 10 US Code 333—Foreign Security Forces: Authority to Build Capacity, 2023. Available: https://www.law.cornell.edu/uscode/text/10/333
27. Chatham House, How Does Capacity-Building Make Cyberspace Better?, 2022. Available: https://www.chathamhouse.org/2022/02/how-does-capacity-building-make-cyberspace-better
28. Office of the Director of National Intelligence, Principles of Professional Ethics for the Intelligence Community, 2014. Available: https://www.dni.gov/index.php/who-we-are/organizations/clpt/clpt-related-menus/clpt-related-links/ic-principles-of-professional-ethics
29. Undersecretary of Defense for Policy, Assessment, Monitoring, and Evaluation Policy for the Security Cooperation Enterprise, 2017. Available: https://open.defense.gov/portals/23/documents/foreignasst/dodi_513214_on_am&e.pdf

Author

Christian Neubauer is MITRE's chief engineer for Europe and Africa Regional Operations. He has worked across the Intelligence Community and the combatant commands on data science and analytic modernization.

Intelligence After Next

MITRE strives to stimulate thought, dialogue, and action for national security leaders developing the plans, policy, and programs to guide the nation. This series of original papers is focused on the issues, policies, capabilities, and concerns of the Intelligence Community's workforce as it prepares for the future. Our intent is to share our unique insights and perspectives surrounding a significant national security concern, a persistent or emerging threat, or to detail the integrated solutions and enabling technologies needed to ensure the success of the Intelligence Community. The views expressed in this publication are those of the author(s) and do not imply endorsement by the Office of the Director of National Intelligence or any other U.S. government department/agency.

Will Scannell, department manager of the strategy and policy department within MITRE's National Security Sector, is the overall manager for the IAN series. He has led development of operational concepts and implementation plans to meet changing strategic, operational, and tactical priorities and presenting strategies to inform policy deliberations at the most senior levels of the government. For questions about the series, Will can be reached at wscannell@mitre.org.

You can receive all of MITRE's Intelligence After Next papers by subscribing to the series at mitre.org/IntelligenceAfterNext

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded research and development centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE
mitre.org

JANUARY 2024