The Case for Creating an Open-Source Intelligence Agency

William Usher

The author is a retired CIA senior intelligence executive. He is now senior director for intelligence with the Special Competitive Studies Project.

Editor's Note: This article was adapted from a response to a request by the Center for the Study of Intelligence, which for the purposes of a panel discussion specified that the author make the case for creating a new OSINT agency. The recommendations do not necessarily reflect the views of the Special Competitive Studies Project or any element of the US government.

The views, opinions, and findings of the author expressed in this article should not be construed as asserting or implying US government endorsement of its factual statements and interpretations or representing the official positions of any component of the United States government.

In 2001, John Gannon—former chair of the National Intelligence Council and deputy director for intelligence at CIA—wrote in this journal that open-source intelligence (OSINT) had become "indispensable to the production of authoritative analysis," yet he noted that the Intelligence Community (IC) faced "an avalanche from both open-source and classified collection sources." He went on to write that, "By itself, the IC simply cannot stay ahead of the technological curve and it knows it."[1]

Almost a quarter of a century later, the promise of OSINT to expand the scope and impact of IC work, as well as the critical challenge the IC faces when working with OSINT—volume, velocity, and veracity—have only become starker. A dynamic ecosystem of national security-focused companies, non-profits, and academia have developed specialized expertise and products by focusing on specific elements of the open-source space. This ecosystem covers nearly every topic of US government concern: human trafficking networks, China's attempts to steal intellectual property from US firms, trends in global public opinion, and nuclear proliferation, just to name a few. The private sector has found tools and strategies to absorb and analyze new data and to push out products at speed.[2]

In this arena, speed to insight—understanding the data faster than others do—is necessary for the United States to respond first to the risks and opportunities the data present. By 2025, it is projected that there will be more than 180 zettabytes of data available, up from 64.2 zettabytes in 2020.[3] Many other countries, including our adversaries, are much less complacent than the IC in leveraging commercially available information (CAI) and/or publicly available information (PAI) for their advantage. For example, China's People's Liberation Army partners with at least five private OSINT providers to collect intelligence on a variety of relevant issues, including foreign military capabilities and deployments.[4]

The IC appears to recognize that integrating data and insights from this world at speed, scope, and volume will be increasingly necessary to continue to offer decision advantage to national security leaders. Solving the IC's OSINT problem has been the subject of many data calls, conferences, academic papers, and op-eds over the past decade. After so many studies, however, an all-encompassing solution has not yet been implemented.

Some senior national security officials believe the way forward remains within the community's current construct. The IC OSINT strategy recently promulgated by the Office of the Director of National Intelligence would appear to support this line of thinking.[a] Others argue that the IC should get out of the OSINT business altogether, on the theory that the government can never match the speed and resources of the private sector and instead should position itself as a good customer of this data. Still others urge a bolder, more transformative approach.

What are We Trying to Solve?

Despite these efforts, the IC is in danger of falling behind on OSINT for a variety of reasons. Taken together, these obstacles are the OSINT problem that any new approach needs to solve, and proposed solutions should be measured by how effectively and efficiently they address these challenges.

The amount of CAI/PAI is exploding, and the IC is not keeping pace to make proper use of it. Data is going undiscovered and underutilized. Relatively few IC officers know what data exists and they

[a] The ODNI's IC OSINT Strategy 2024–2026 defines OSINT as intelligence derived exclusively from publicly available information or commercially available information that addresses specific intelligence priorities, requirements, or gaps.

face myriad financial, security, and bureaucratic obstacles to obtaining it. Even if they succeed, IC officers often lack the data management and OSINT tradecraft skills or access to cutting-edge analytic tools to effectively utilize the data.

The IC has a poor understanding of the data it holds, how valuable it is, where it is kept, and how it is used. The new DNI OSINT strategy admirably calls attention to these shortcomings, but IC agencies are still not incentivized or required to share the CAI/PAI they have acquired and the Community often pays multiple times for access to the same data. This challenge is compounded by the extremely dynamic nature of the global data market, which continues to grow exponentially in aggregate but with a great deal of volatility. The quality and availability of individual datasets are constantly shifting; commercial vendors rise and fall; datasets are created, then bought and removed from circulation, or priced expensively; academic-created datasets are often closely held so that the original creator can fully exploit it before making it more accessible; adversaries are closing off access to their domestic data ecosystems while they actively try to pollute our datasets.

While it is generally less expensive and risky for the IC to gather open-source data, the IC under invests in OSINT capabilities in favor of its more traditional collection capabilities and methods. Existing OSINT entities, such as CIA's Open Source Enterprise, are subordinated within existing bureaucratic structures, impeding their ability to harness resources and exert influence.[5]

As a consequence, even as policymaker demands on the IC for intelligence insights continue to increase, the IC fails to deliver OSINT-derived assessments and other products at scale and at speed. Because the IC generally relies on its all-source analytic cadre to filter the assessments that reach its seniormost customers, and because most IC analysts remain relatively poor consumers and users of CAI/PAI, OSINT-derived insights often do not reach key decisionmakers in a timely fashion, if at all. Moreover, the IC's small cadre of dedicated OSINT analysts are not well-integrated into all-source analytic teams.

The Case for a New Agency

To fully address the OSINT problem and maintain the IC's relevance and strategic edge with decisionmakers, the United States should create a new, 19th agency within the IC dedicated to the task. The new Open Source Agency (OSA) should be a standalone and independent member of the IC; its principal purpose would be to acquire, curate, develop, employ, and share CAI and PAI data sources for intelligence purposes.

At least initially, its function would be to deliver OSINT to other IC members (and, selectively, to foreign allies and partners, the private sector, and to the public) for them to analyze and make use of. Just as the National Reconnaissance Office builds and operates the US constellation of satellites but relies on the National Geospatial-Intelligence Agency and other IC agencies to analyze the data they collect, OSA would focus on accelerating and streamlining the acquisition of PAI/CAI that other agencies would make use of.[6]

OSA employees would "live" in the unclassified realm, spending much of their time in unclassified workspaces and on low-side unclassified systems, freeing them up to have regular access to and collaboration with the private sector. As with In-Q-Tel, OSA would have designated secure spaces for classified work and secure communications with the rest of the IC to solicit intelligence requirements, disseminate information, and collaborate on classified projects to include targeting studies and collection planning.

OSA would be established using IC authorities and would become the IC's "functional manager" for OSINT in the same way the NSA director is the functional manager for SIGINT and the CIA director (DCIA) is the functional manager for HUMINT. OSA's director would report to the DNI, and it would be subject to congressional oversight by the HPSCI and SSCI and have its own budget appropriation.

OSA would apply and enforce ODNI-established standards for incorporation of CAI/PAI data with regards to privacy and security compliance, quality, IC-wide availability, and pricing. OSA would act as the contractor and go-between connecting data vendors with IC agencies, which would store and analyze the take.

OSA would ensure consistency, interoperability, and life-cycle monitoring and accounting for CAI/PAI datasets that were acquired, and it would be responsive to NIPF priorities and IC requirements and tasking. It would offer commercial vendors a reliable one-stop point of entry to sell their data and analytic tools to the IC, making it easier and more efficient for the private sector to partner with the IC. Because it would look across IC equities and requirements, OSA should be able to exert its market power to drive down costs and increase interoperability and access to commercially-developed solutions.

OSINT Tradecraft

OSA's second principal mission would be to cultivate, develop, and teach OSINT tradecraft to elevate the acumen of the entire IC. OSA would have the IC's experts on the CAI/PAI information domain—including the commercial marketplace, vendors, datasets, and commercially sold analytics and platforms. OSA would become the data partners to the IC's cadre of all-source analysts and collectors, helping them incorporate OSINT to meet mission requirements.

OSA's capabilities would be available to all the other 18 IC agencies and would include acting as the IC's trusted evaluator of commercial tools and platforms, and the focal point for CI and supply-chain vetting of commercial data vendors and their capabilities. OSA, for example, could maintain the IC's catalog of proven and vetted commercial datasets that IC agencies could tap into when mission requirements demand. Eventually, OSA could develop AI-driven API platforms to integrate valued datasets and simplify the process for IC agencies to tap into them.

It could also act as the IC arm for discovering, evaluating, and advertising open source-derived assessments by the private sector (commercial vendors, academics, or think tanks experts) of relevance to US national security priorities. It could publish a regular compendium of the best commercial OSINT tradecraft and tools (including data management, visualization, augmented and virtual reality, and storytelling) to educate other IC offices and promote their use.

As it matures, OSA should develop in-house analytic capabilities, focused on topics that most readily lend themselves to unclassified open sources, such as politics and foreign policy, transnational issues, economic trends, or technology assessments. At the direction of the president, ODNI, and DCIA, the Open Source Agency could further develop cloud-based unclassified online collaboration spaces to enable broader IC analytic outreach with the private sector, state and local authorities, foreign intelligence liaison services, and the general public.[7]

While other options for solving the OSINT problem have their individual merits, creating a new dedicated agency offers the best, achievable, and sustainable path for success. It is the one solution that would give OSINT greater stature across the IC and better enable Congress and the White House to direct greater resources toward it. Because the new agency would not produce assessments, this approach would avoid creating duplicative and wasteful analytic capabilities and minimize the chances of debilitating bureaucratic infighting for analytic access to policymakers while OSA and its IC partners determine where its analytic capabilities are best deployed.

Maintaining the all-source analytic community's purview over the delivery of insights to policymakers also keeps the intelligence "conversation" with senior intelligence customers focused and vibrant. In this author's experience, customers rarely demand unclassified assessments and instead want the best analysis using whatever sources are available. Development missions would be made available IC-wide to enhance the work done by all-source analytic units.

Just as the NRO influenced the direction of commercial space development to ensure US national security requirements were prioritized and addressed, so would OSA for OSINT. As the IC's OSINT functional manager, OSA would have the writ and budget to identify, acquire, and promote which CAI and PAI sources the IC should acquire. Organizing OSINT efforts under OSA would give the IC greater market power to generate supply of relevant CAI and spur innovation in the private sector. In the long run, it would be cheaper and more efficient to do this in-house.

As it gains experience and proves its worth, OSA would be positioned to drive OSINT resources and tradecraft forward, enlarging and accelerating OSINT's ability to close intelligence gaps and deliver strategic insight, thereby allowing for more efficient use of classified collection capabilities and reserving them for the truly hard targets that only they can penetrate. OSA would be an ideal sandbox for the IC to experiment with large-language models, other forms of generative artificial intelligence, and machine learning tools, applying them to deliver intelligence insights in new and innovative ways.

Oversight

The White House would need to request, and Congress would need to authorize and appropriate funds to establish a new agency. It probably would take considerable time to hire and onboard staff and identify suitable physical space. One way to speed up the process would be to identify certain roles within OSA that would not require a security clearance, or a basic secret-level clearance. To be fully successful, OSA would need to be invested with requisite authorities over the application of OSINT and enjoy sufficient standing in the IC to deliver insight to customers.

Just as Executive Order 12333, the Foreign Intelligence Surveillance Act, and National Security Directive 42 authorize NSA to collect foreign signals intelligence and protect national security systems, OSA would need strong executive authority to approve, modify, or disallow CAI/PAI acquisitions across the IC. Agencies would need to be incentivized (and, in turn, create incentives for their officers) to make better use of CAI/PAI data and to adopt OSA's recommended tradecraft.

As its analytic capabilities grew, OSA would need an online dissemination capability, along with representation on the President's Analytic Support Staff to feed into the PDB process and at the National Intelligence Board to contribute to the production of national intelligence estimates.

OSA would need empowered, layered, and independent oversight mechanisms to ensure compliance with US law and established IC privacy protection practices. In line with other IC agencies, OSA's inspector general should be a presidential appointee confirmed by the Senate; the IG should report regularly to the White House and to Congress on OSA's performance and handling of PII compliance. Finally, the ODNI's Office of Civil Liberties, Privacy, and Transparency should conduct regular, independent reviews. ■

Endnotes

1. John Gannon, "The Strategic Use of Open-Source Information," *Studies in Intelligence* 45, No. 3 (September 2001).
2. See Jami Miscik, Peter Orszag, Theodore Bunzel, "Geopolitics in the C-Suite," *Foreign Affairs*, March 11, 2024.
3. Petroc Taylor, "Amount of Data Created, Consumed, and Stored 2010–2020, with Forecasts to 2025," *Statista*, November 16, 2023. https://www.statista.com/statistics/871513/worldwide-data-created/.
4. Zoe Haver, "Private Eyes: China's Embrace of Open-Source Military Intelligence," *Recorded Future*, June 1, 2023. https://www.recordedfuture.com/research/private-eyes-chinas-embrace-open-source-military-intelligence.
5. Cortney Weinbaum, Bradley M. Knopp, Soo Kim, Yuliya Shokh, "Options for Strengthening All-Source Intelligence: Substantive Change is Within Reach," RAND Corporation, February 28, 2022.
6. This concept was first put forward by Kevin Johnston in "It's Time to Give OSINT Its Own Agency," *Fair Observer*, February 25, 2022. https://www.fairobserver.com/region/north_america/kevin-johnston-osint-us-intelligence-community-internatinoal-security-news-35271/ [sic].
7. For more on IC's partnerships with state and local authorities, academia, the private sector and the public, see the description of "intelligence as a service" for the US public in Weinbaum, et al., *Options for Strengthening All-Source Intelligence.*■