Debating How the IC Should Approach Open Source Intelligence

A Roundtable Discussion

John Pulju

John Pulju is director of the Center for the Study of Intelligence and chair of the *Studies in Intelligence* Editorial Board.

Experts have been debating how the US Intelligence Community should approach open-source collection and analysis for decades. This debate has intensified as the information revolution has gathered pace. Commentators have advocated for approaches ranging from creating an open-source agency to relying almost entirely on the private sector. The debate may even intensify as artificial intelligence (AI) capabilities expand and the IC's budget environment tightens. In this context, a group of two dozen IC and private sector open-source practitioners

and thinkers met in June 2024 to discuss four possible approaches. The roundtable began with opening remarks by this author and IC OSINT Executive Jason Barrett, who both noted the event was intended to compare the approaches and tease out assumptions, tradeoffs, and practical implications—such as resource needs—that would help future decisionmakers grapple with how to proceed.

Roundtable Speakers

Sam Gordy is President, Janes Group U.S. with 40 years' experience working with defense, intelligence, and civilian government customers in the United States and abroad. Before joining Janes in 2023, Sam spent the bulk of his career at SAIC-Leidos and five years with IBM. Throughout his career he has focused on providing clients with information technology products, services, and solutions in areas ranging from cyber security to exploiting cognitive systems. He has served as an adjunct lecturer at Georgetown University and began his career as an intelligence officer in the US Navy.

Emily Harding is Director of the Intelligence, National Security, and Technology Program at CSIS and Deputy Director of the International Security Program. She has served in a series of high-profile positions, notably including Deputy Staff Director of the Senate Select Committee on Intelligence, Director for Iran on the National Security Council Staff, and Deputy Chief of CIA's Iraq Group during the attempted ISIS takeover. She is an adjunct lecturer at the Johns Hopkins School of Advanced International Studies.

William "Chip" Usher is Senior Director for Intelligence at the Special Competitiveness Studies Project. Prior to SCSP, Chip served 32 years at CIA, where he held a variety of executive positions and was a member of the Senior Intelligence Service. He has expertise on East Asia, the Near East, and Eurasia as well as IC modernization. He is passionate about enhancing the IC's ability to provide timely, relevant intelligence insights to US decisionmakers. Before joining the US government, Chip ran an import-export company in Nagoya, Japan.

Kristin Wood is CEO and Co-Founder of August Interactive, a deep-tech start-up that is building immersive games and experiences. She serves on the advisory boards of numerous tech start-ups and venture capital firms. In her 20 years at CIA and in the Senior Intelligence Ser-vice, she served as a PDB briefer, led the team assessing whether Iraq had a role in the 9/11 attacks, and was a Deputy Chief of a Middle East division in the National Clandestine Service. In her final CIA posi-tion she served as the Deputy Director of Innovation and Technology at the Open Source Center.

Four Approaches

Private-sector thinkers who also have extensive experience in the IC and US government took the lead in laying out the case for each of the approaches. Following this, Randy Nixon, the director of the Open Source Enterprise (OSE), engaged the speakers and other participants in a wide-ranging discussion. To aid debate, CSI asked the speakers to push the bounds in making the case for each approach while also addressing pros, cons, and tradeoffs. Speakers and other participants understand there are many potential variants of each approach as well as the possibility of mixing and matching elements.

Reinforce Federated Programs

Emily Harding made the case to reinforce current IC programs, centered around OSE leading a federated IC-wide effort to aggressively implement the new OSINT strategy. This approach would expand use of AI tools like OSIRIS to summarize, translate, and disseminate open-source data, including identifying source biases and identifying new insights. Dissemination of OSINT products would be across the IC and beyond. She noted the ODNI OSINT strategy hits the right key areas: structuring and sharing data; developing data-science tools and rigorous tradecraft standards; and integrating open source fully into the IC's work, particularly all-source analysis. She argued this approach is preferable to creating an Open Source Agency (OSA), which would be disruptive as it stood up and create more complexity in an already sprawling IC.

She also assessed it would be no more likely to receive adequate resources or authority than current IC components—both of which she believes need to be increased. The federated approach also offers flexibility for IC components to tailor their OSINT activities to needs ranging from tactical support to combat forces to all-source assessments for national-level policymakers.[a]

Adopt a Surgical Approach

Kristin Wood argued that the IC should create a non-profit Public-Private Consortium to leverage the rapidly growing number of firms, individuals and organizations that are exploiting the explosion of information.[b] With digital information now counted in zettabytes—one trillion gigabytes—across a dizzying array of media the IC cannot hope to keep up with the thousands of entities that have emerged to capture and analyze it. Instead, the consortium would leverage what has become a $58 billion industry to glean what the IC needs to accomplish its mission. The consortium would scan the horizon for useful content and tools. It would foster common tradecraft standards among its members, vet sources, set prices, and provide data to components across the IC. It might create an automated OSINT feed—a *Drudge Report* for the IC—and could broker ad hoc taskings and data acquisitions. Wood noted that

The IC OSINT Strategy, 2024–2026

The Strategy aims to build an integrated and agile OSINT community that can extract insights from the vast amounts of open source data to both deliver unique intelligence and enable other collection disciplines.[1] It terms OSINT "the INT of first resort" and defines it as "intelligence derived exclusively from publicly or commercially available information that addresses specific intelligence priorities, requirements, or gaps." The Strategy aims to bolster IC effectiveness in the current federated approach with the DCIA as the Functional Manager while also boosting partnerships with industry, academia, and foreign counterparts. It lays out four areas of strategic focus:

- Coordinate Open Source Data Acquisition and Expand Sharing. Avoiding redundancy and expanding sharing of open source data and tools are priorities, as are ensuring the most efficient use of IC resources.
- Establish Integrated Open Source Collection Management. A priority is developing processes, tools, and metrics to align collection efforts to ensure they meet priority needs, cover gaps, avoid duplication—including with sensitive collection efforts–and comply with privacy and civil liberties.
- Drive OSINT Innovation to Deliver New Capabilities. A priority is accelerating development and adoption of tools to exploit open source data and information, particularly in areas like AI, machine learning and human language.
- Develop the Next-Generation OSINT Workforce and Tradecraft. Priorities include establishing common tradecraft standards needed to exploit the digital environment, updating them regularly, and training both a cadre of highly skilled OSINT specialists and the IC workforce.

CIA's Open Source Enterprise executes the DCIA's responsibilities as Functional Manager. CIA leads the National Open Source Committee, an IC group that shares best practices, identifies gaps, and develops joint solutions to common challenges. The Committee has made notable achievements in areas like aligning and deconflicting purchases of CAI, building an inventory of OSINT tools and technology, and establishing common tradecraft and training.

a. OSIRIS is an OSE tool available to the IC that applies generative AI to develop insights from a wide range of open-source material. It reached initial operational capability in 2023.

b. William Usher also advocates for a consortium, which could be tied to an Open Source Agency. For further details, see Wood and Usher's article, "The Intelligence Community Can Tackle Open-Source Data in a Hyper-Connected World," *Cipher Brief*, December 21, 2023, and "Intelligence Innovation: Repositioning for Future Technology Competition," Special Competitive Studies Project Interim Panel Report, April 2024.

keys to success would be flexibility, agility, and "living" in the open-source world. The Consortium would be small—$20 million might be enough to operate it, at least initially.

Rely on the Private Sector

Sam Gordy advocated privatizing the overwhelming bulk of OSINT collection and analysis. He argued that the information revolution has given the private sector capabilities not only in areas like social media and AI, as Harding and Wood argued, but also in areas that historically were restricted to government, such as IMINT and SIGINT. At the same time, commercial analytic capabilities have matured to "turn open-source information into OSINT." He argued that relying on the private sector would reduce costs, whether for people or facilities. It would offer an increased ability to surge globally and take advantage of cultural expertise, language skills, and real-world experience with the systems, doctrine, and tradecraft of our adversaries. He said challenges include counterintelligence and OSINT tradecraft—including detecting disinformation—and linking to the classified "high side." Firms that specialize in OSINT, however, are able to overcome these challenges through coordination with the IC and other government customers.

Create an Open Source Agency

William Usher made the case for consolidating IC OSINT programs and resources in an Open Source Agency (OSA). He argued this would be surest path to ensuring the necessary funding is devoted to OSINT, to developing a sizable cadre of officers who are skilled in "living" in the open-source world—most would not have security clearances—and to giving open source a strong voice in driving how the IC will satisfy intelligence requirements. OSA's primary purpose would be to quickly obtain, curate, and share commercially and publicly available datasets across the IC. It would be the "one stop" shop for commercial vendors, set standards for incorporation of OSINT data, and evaluate platforms and tools to get and exploit it. Like NRO for overhead collection and NSA for SIGINT, it would have authority to approve and guide any individual agency OSINT efforts. As it became established, OSA could also add in-house analytic capabilities and develop unclassified collaboration spaces with US and foreign partners. And, it would work with other IC officers to incorporate OSINT into all-source products while training them in basic techniques—"teaching them to fish." [See Usher's separate article in this edition of *Studies* for more details on his proposal.]

Key Themes

The speakers and other participants agreed that whatever approach the IC takes, it needs to improve its exploitation of open source. Much of the debate was about resources and how to change the culture of the IC so that OSINT could become truly the "INT of first resort." Beyond the basic differences among the four approaches, participants suggested different ways to tackle this goal. The debate also revealed differing approaches to topics like security and clarified some choices decisionmakers would need to make if they decided to pursue one or more of the approaches.

Untapped Potential

The speakers and other participants in the roundtable all agreed that the Intelligence Community is not taking enough advantage of OSINT. They added that urgent action is needed. IC OSINT executive Jason Barrett said that OSINT could satisfy 60–70 percent of US intelligence requirements. Brad Ahlskog, director of DIA's OSINT Integration Center (OSIC), suggested the share might be as high as 80 percent. Nixon said the gap between what the IC is doing and could be doing is growing because funding does not match the ability of the IC to take advantage of commercially available information (CAI). Usher echoed this view, noting that the explosion of data is the story; both

Approach	Features	Resources	Practicalities & Areas to Clarify	Arguments For	Arguments Against
Federated	Drive IC OSINT Strategy Keep Separate Components OSINT Champion (Directorate?) Set Standards, Tradecraft Expand OSINT Dissem	More Funds More People	AI Critical–Tools, Skills	IC on Right Track Already Minimal Disruption of Change Components Can Tailor to Needs Protects Security/ CI Meets Consumer Need	Informal authority insufficient Doesn't make OSINT equal "INT" Local decisions hurt efficiency, quality Components raid OSINT resources Feckless to compete with private sector
Consortium "Surgical"	Public-Private 501c3 Scan horizon for data, tools Build Partnershps Foster standards, sharing One-stop shop to reach IC	$20 million to run A few IC officers 20-30 private sector	Highly flexible on size, topics Could fit with other approaches POC for procurement?	Keeps up with Info Revolution Ingest, acquire only what needed Cost–federated buying Private sector entre to IC	Minimal impact if small Cost savings unclear Greater CI, security concerns Drift into topics of marginal FI value Potential privacy issues Privatization Outsource
Privatization	Outsource almost all OSINT Most collection, analysis private IC focus on sensitive collection Components drive what needed	Fewer IC officers More Funds	Keep small IC unit for niche topics How to organize procurement	Cost–unclassified cheaper Ingest, buy only what needed Flexibility – surge, tailor to user Eases privacy issues	Cost savings illusory (profit) Deconflicting procurements & ops No objective IC OSINT experts Creater CI, security concerns
OSINT Agency	Consolidate OSINT in new Agency Director OSINT Champion Set standards, tradecraft Emphasize acquiring, sharing Control procurement funds	Large 2000-3000 people Billion $+	Authority over other IC agencies Cost–Federated buying Promotes quality Deconflict security, CI issues	Elevates OSINT as Equal "INT" Cost–Federated buying Promotes quality Deconflict security, CI issues	New IC stovepipe; overlap with others Long, disruptive period to create Feckless to compete with private sector Components lose ability to tailor to needs

he and Wood said the US is getting crushed by China, Russia, and other adversaries that are investing heavily in exploiting OSINT. Gordy agreed with this.

The speakers commented that former IC officers are often stunned by the volume and variety of OSINT that is available. Harding gave an example of a 1,000-page SSCI report on Russian election meddling that drew on a million pages of open-source material. She also noted that the social media platform X provides early detection of events ranging from natural disasters to the US raids that killed Usama bin Ladin and ISIS leader Abu Dua. Wood flagged the growing importance of virtual reality for communications, relationship building, and even business. She said the IC has barely tapped this "fusion world" and needs to understand it to avoid surprise. Gordy noted the proliferation of private intelligence, marketing, and other firms that are exploiting "adtech," commercial imagery, and other open sources to track the war in Ukraine. The speakers also stressed the utility of OSINT in providing timely insights to US officials and partners. Harding commented that it offers the potential to provide instant delivery via mobile devices to intelligence consumers anywhere, anytime. Several participants cited the advantages of OSINT in allowing the IC to push insights to foreign partners, local governments, and the public. They see this as a growing part of the IC's mission.

Coverage

The four approaches emphasize different aspects of open source and different roles for IC OSINT components. All focus on digital data generated by the information revolution—both the mass of data and metadata available in social media, virtual reality, the "internet of things," and elsewhere as well as the tools that have been developed to extract intelligence from digital information, ranging from basic search tools to AI applications. However, the IC would probably end up ingesting and processing much less digital information under the Privatization and Surgical approaches because these rely much more heavily on the private sector to extract insights.

Privatization would also give greater weight to commercially available imagery, SIGINT, HUMINT, and all-source analysis. Gordy termed OSINT "the INT of INTs," echoing views Mark Lowenthal expressed in his 2001 *Studies* article about how open-source information is pervasive with other INTs.[a] He gave examples of Jane's global network of employees—essentially providing open-source HUMINT. Participants also noted the ability of firms and people to track battlefield movements in Ukraine and Gaza with commercial imagery and "adtech." Gordy argued that the IC should concentrate on areas where clandestine and other sensitive collection are truly needed. He said clandestine HUMINT should the INT of last resort, given the risks to the people involved.

None of the speakers discussed where the boundary would be defined between OSINT and other unclassified IC activities, such as internet research, analytic outreach, or purchase of CAI. The discussion suggested they would want to minimize overlap and conflict, while recognizing that boundaries might be fuzzy. Usher, for example, proposed that an OSA would only gradually begin producing analytic products to minimize conflict with all-source agencies. (Ahlskog and Nixon noted that their components already produce OSINT-only analytic products.) Privatization might ease the problem by leaving it up to a wide range of IC components to decide what activities to retain and what to outsource.

Nixon commented that many participants are defining OSINT narrowly as social media or that which is only digital. He noted

a. Lowenthal wrote, "OSINT is the most pervasive of the INTs, rather than a separate category. It occupies its own niche as well as some part of each of the other INTs (HUMINT, IMINT, MASINT, SIGINT). Beyond the textual sources of OSINT, the only aspect that differentiates it from other collection disciplines is the fact that it is not clandestine in nature." "OSINT: The State of the Art, the Artless State," *Studies in Intelligence* 45, No. 3 (September 2001).

Studies *Articles on Open-Source Intelligence*

Open source has been a recurring topic in *Studies in Intelligence* from the 1950s through today, including most recently roundtable participant Chris Rasmussen's article (June 2024) on the need for an open-source agency. Early articles highlighted the amount and variety of open sources as well as their importance, particularly in the absence of other intelligence on hard-target countries. J.J. Bagnall (1958) and David Moore (1963) detailed open sources including "gray literature" (not quite public, not quite secret) to periodicals, books, radio, television, émigrés accounts, and Western academics. They describe these sources as "many and varied." Open sources accounted for the majority of intelligence on such topics as Soviet military doctrine, weapons programs, research and development, and order-of-battle. Both authors noted challenges that persist today—lack of foreign language and translation services, the scattered nature of sources, the difficulty of validating materials, and the need to process vast amounts of data.

Although the increasing availability of satellite photography undoubtedly reduced the IC's reliance on open sources for Soviet military topics, Herman Croom (1969) noted they were still important—often providing the first indications of research and development of military significance—as well as being key in other areas, such as leadership plans and intentions. Gail Solin (1975) stressed not only the criticality of open sources but also the development of "Sinology" and "Kremlinology" to tease insights from fragmentary and opaque sources. For example, she noted that counting uniform pockets was a key to identifying officers in the People's Liberation Army after insignia were abolished during the Cultural Revolution. Croom and Solin both emphasized the need for deep expertise to make sense of open sources and cut through propaganda—what today might be termed disinformation. Croom also dwelt on implications of the information explosion—an explosion that the IC has seen as both an opportunity and a challenge ever since.

As the Cold War gave way to 24/7 cable news, commercial satellite imagery, and the "cyberworld," David Gries (1991) and David Overton (1992) saw open sources as critical to intelligence during the 1990s. Gries argued that open sources already provided 80 percent of analysts' information and that this would grow. Mark Lowenthal (2001), John Gannon (2001), and Stephen Mercado (2004) continued this theme in their articles of the early 2000s; they stressed the need to develop ways to collect and process the huge amounts of data that were being made available by the internet and to develop strong tradecraft for OSINT—a term that had come into vogue. Many of their recommendations on organization, resources, and tradecraft resonate with the debate that continues today. Among many other articles that touch on OSINT, one with particular relevance is Marty Petersen's argument (2003) that effective political analysts must have language skills and deep country knowledge—in his case, China—to ensure they can exploit open sources.[2]

that the vast amount of publicly available and often most useful data remains print, broadcast, and radio. He speculated that this publicly available information (PAI) is often taken for granted because OSE and its predecessor FBIS have provided it to the IC free of charge since 1941. He noted, however, that collection, processing, and analysis of this PAI require large resources.

Resources

There was general agreement that the IC needs to devote more resources to OSINT, whether to acquire, process, and share open-source material or to develop AI and other tools to extract insights from it. Wood commented that OSINT will not be the INT of first resort unless it is resourced that way. Barrett described the 2010 to 2020 period as a "lost decade" from a budget perspective as fewer IC components associated their activities with OSINT even amidst the rapid growth and value of commercial information. Nixon added that budgets devoted to OSINT have actually been declining even amidst the information explosion. Both Barrett and Nixon acknowledged that there may be other spending on open source that is captured in budgets as something else—e.g., publication or data procurement.

There was less consensus about how much more the IC needs to invest in OSINT. The varied approaches suggest large differences in financial and human resources. Several participants argued that producing OSINT is inherently less expensive than clandestine human and technical collection and that their recommended approaches would make it even more efficient.

Gordy argued that privatization would provide large cost savings. Companies operating at the unclassified level have far lower personnel and security costs than IC components and could rapidly surge to provide tailored OSINT in response to US government needs, which would reduce fixed costs of maintaining large programs covering topics or countries "just in case." Wood's consortium concept incorporates some of these features and also offers the potential that participating firms and organizations would provide some OSINT to the IC free of charge. Usher's version of an OSA might offer some of the same savings, given that it would operate largely at the unclassified level and have a mainly uncleared staff. Several participants argued that the IC could cut the costs of acquiring CAI by centralizing procurement.

Other participants who have experience in acquiring open-source data were skeptical that major gains in OSINT could be made without large increases in spending, particularly on CAI. Nixon and Ahlskog noted that they already cannot afford all the CAI that IC components want to exploit and that previous efforts to drive down costs by centralizing procurement have had little success. Privatization also might cost more as the IC would be paying for PAI it now collects on its own. That said, they believe significant increases in greater spending on OSINT would be worthwhile because it provides more bang for the buck than other INTs. Reducing spending on other INTs to increase spending on OSINT would improve the IC's ability to meet customers' intelligence requirements.

There was little discussion about human resources, but the varying approaches might drive sharply different requirements—some might even lead to IC cuts. Reinforcing the current IC approach implies increasing the number of OSINT specialists. Similarly, Usher suggests an Open Source Agency would need 2,000–3,000 people; some would be transferred from CIA and DIA. By contrast, the Privatization approach raises the potential of sharp cuts in OSE, OSIC, and other IC components.

Authorities

There was a strong consensus that OSINT practitioners need more authority to compete with other INTs in resource allocation and other decisions, such as balancing openness and security. All speakers called for a clear, strong OSINT leader—"a champion" or "the person" overseeing OSINT. They saw a need for this champion to advocate for OSINT across the IC, Congress, and the public.

Speakers said that the DCIA, as functional manager of OSINT, has too many other responsibilities to be the champion. Harding argued that symbols and rank matter in Washington and that this was more important than formal authority over IC budgets and programs. She suggested elevating OSE to the directorate level—making its chief a direct report to the DCIA and a peer of the chiefs of its operational and analytic components. An alternative would be to create a presidentially appointed, Senate-confirmed position in ODNI. In contrast, Gordy argued that an OSINT leader should have the formal authority to move resources. Usher agreed; he would centralize most funding and people in OSA and give its director authority to approve open-source activities by other IC components.

Culture

The discussion on authority reflected another area of consensus: all participants emphasized that major change in IC culture would be needed to take advantage of OSINT's potential. Although the IC OSINT Strategy calls for it to be "the INT of first resort"

participants noted a pervasive emphasis across the IC on clandestine collection of all sorts. One argued that most all-source analysts gravitate to HUMINT and SIGINT and lack the language skills and substantive expertise to fully exploit open source. This is true even though for decades open sources have often been the dominant source of intelligence. Some participants see a "not invented here" attitude to OSINT as well as a bureaucratic impulse among components to contribute secretly acquired intelligence even when it is not needed.

One participant commented that OSINT officers are treated as "second-class citizens." Their contributions are belittled as "clipping newspapers," rather than seen as making sense of huge datasets. Elsewhere, officers have noted that the needs of other INTs are given priority; for example, in engagement with outside experts and private firms. Another participant commented that the bias can be subtle. He said that templates to source PDBs and other products, for example, encourage listing only a few sources and favor those that have been "serialized"—formally disseminated. Not surprisingly, analysts and editors typically list a few secret, serialized sources rather than a large number of OSINT sources, many of which are not formally disseminated. Nixon noted that OSE is increasing its dissemination of serialized products. Other participants said that the OSINT enterprise lacks a compelling product line for decisionmakers.

Harding suggested some ways to change the culture, most of which could be done under any of the four approaches. These including having the "champion" regularly tout OSINT successes that would resonate with Congress and the public. Successes could range from breaking new substantive ground to saving money or expanding public-private partnerships. She also suggested that deploying "rock star" OSINT officers to other components would increase IC officers' respect for the discipline, while expanding work-from-home options for OSINT employees could attract high-quality experts. Usher suggested that a major advantage of creating an OSA would be elevating respect for its officers; if nothing else, its director would be a peer of other agencies' directors.

Participants discussed the potential that giving IC components "budgets" to buy OSINT would promote its use across the IC. Reflecting their view that IC officers devalue OSINT, most were skeptical that this would work. They worried that components would find ways to divert OSINT funds to other purposes and noted that fee-for-service models have a poor track record of success in the IC. This view also suggests that broad cultural change would be particularly critical to the success of the Privatization and Surgical approaches if these involved a large shift of resources from current IC OSINT components. In these cases, funding would depend on other components' views of the value of OSINT.

The speakers and many participants argued that there is less need for cultural change among consumers of intelligence—policymakers, military and law enforcement officials, and others. They live for the most part in the open-source world and want intelligence they can use and share widely. Participants commented that consumers' key concerns are accuracy and timeliness.

A few participants were more skeptical, citing consumer comments that suggest what they most value from the IC is clandestine human and technical reporting—the "good stuff," as President George W. Bush once put it. Nixon commented that there is a tendency for new administrations and officials to want the "good stuff" early in their tenures, but that this fades as they gain experience. They learn to recognize when they do and do not need precise or highly reliable intelligence that can be gathered only clandestinely.

Tradecraft

Most of the speakers and several other participants stressed that the IC needs to expand its cadre of experts with strong

OSINT tradecraft skills. Harding and Usher, echoed by Nixon and Ahlskog, argued that this cadre should be concentrated in components that are dedicated to OSINT. The cadre would also have the responsibility to set standards for OSINT tradecraft, to teach at least the basics to other IC officers—"teach them to fish"—and to team with them on joint projects. One participant commented that this would help deal with the numerous "OSINT amateurs" around the IC. Gordy and Wood also stressed the importance of tradecraft, although it was not clear whether the number of IC OSINT specialists would increase or decrease under the Privatization and Surgical approaches.

Discussion on tradecraft concentrated on two areas: discovering, processing, and sharing data; and, validating information. Participants commented that much of the huge volume of digital data needs to put into a form that is exploitable before any intelligence value can be gained. Harding and Usher cited the need to structure or curate data. Ahlskog commented that DIA put its OSINT unit in its technical-data–collection directorate because the officers' skills fit better there than in an analytic unit and doing so helps minimize analytic biases. On validation, speakers and other participants saw spotting disinformation or misinformation was one challenge; another is understanding the sources to be able to judge their access and credibility. Nixon noted that a key element of OSINT tradecraft is learning techniques to discover useful data, particularly data that may not be readably discoverable.

Gordy said Janes and other private firms have developed rigorous OSINT tradecraft that parallels many IC best-practices in scoping an intelligence problem, determining how to solve it from available and potential sources, validating and fusing reporting from different sources, and preparing a final report. Gordy sees this tradecraft as key to giving governments confidence in outsourcing OSINT. He noted that Janes has developed criteria for rating the access and credibility of some 700 people who provide it information, including keeping a track record of their reliability. Gordy, Wood, and other participants also commented on the skill firms, individuals, and organizations like Bellingcat have developed to extract intelligence from digital sources.

None of the speakers or other participants discussed overlap between OSINT tradecraft and data science or other "tradecrafts," such as targeting, GEOINT, or all-source analysis. Clarifying the core elements of OSINT tradecraft might help change IC culture by highlighting its distinct value. (In his article for *Studies* in June 2024, Chris Rasmussen argues for a professionalization of OSINT. He addresses some aspects of tradecraft, although he does not use the term.)

Security and Counterintelligence

Security and counterintelligence came up as concerns throughout the discussion. Participants expressed differing levels of concern about the risks, whether to the ability to collect OSINT or to the safety of people who collect it. These views had implications for which approach they favored. In general, the greater the perceived risks, the more likely participants were to favor retaining robust IC open-source components with cleared staff.

Some speakers argued that the overwhelming amount of CAI and PAI already has made it almost impossible for any government, organization, or firm to hide all but the most sensitive secrets, greatly reducing the need for clandestine collection. Technical barriers like China's "Great Firewall" present challenges but there are myriad avenues to get needed intelligence, mitigating the risk of discovery and of damage if one is lost. Other participants were more skeptical of the availability of digital information, particularly on topics of priority intelligence interest, and of the ability of non-government actors to get more sensitive data without tipping the owner. Jonah Victor's article in this edition of Studies on diminishing access to information in China suggests that

adversaries may increasingly avoid exposing sensitive information digitally, forcing more OSINT into a gray area more closely resembling clandestine collection.

Gordy expressed confidence in the personal security of people who provide information to Janes and other firms around the world. Several other participants suggested he was underrating the individual risks, including blowback on the US government if private citizens were arrested for undertaking what would seem to other countries like outsourced espionage. The risks extend beyond HUMINT; private cyber efforts could invite retaliatory cyberattacks or even physical attacks on hackers, for example. Targets also might respond by taking security measures that would cut off access to other intelligence streams.

All participants saw the handoff between the unclassified and classified domains as a manageable challenge. With the exception of proponents of reinforcing the IC's Federated Approach, they all favored having OSINT practitioners "live" as much as possible in the unclassified world, to include not having security clearances. They acknowledged that securely passing intelligence requirements from the classified to the unclassified domains would be a challenge but thought this should not be overstated; one participant quipped that it would take about 10 minutes for a person to guess the topics on the National Intelligence Priorities Framework. OSINT collectors could take measures to obscure priorities, although doing so would increase cost.

CI and security challenges would be most muted in the Federated Approach. Current OSINT officers are fully cleared. They can work with other IC officers on the handoff challenges and are well positioned to deconflict with other IC components when OSINT and clandestine activities might intersect.

Privacy and Civil Liberties

All participants agreed that it is critical for policymakers to decide where to set the line in the inherent conflict between protecting US persons' privacy rights and fully exploiting digital information. This is a decision for the White House and Congress. It goes beyond the debate over Section 702 authorities in the Foreign Intelligence Surveillance Act, which will be up for renewal in two years, to the implications for privacy of AI, the internet of things, and other advances in technology. Where policymakers draw the line will have implications for which approach to OSINT they want the IC to pursue.

Wood argued that the IC needs to have access to CAI that contains US persons data to ensure the United States has the intelligence it needs to compete with China and to tackle challenges that cross borders, such as counterintelligence, human and narcotics trafficking, and technology. US firms—and even US adversaries—have access to this data, which is critical to drawing insights from the massive amounts of digital information that is available. She added that major US firms want to help tackle the challenges and suggested they might help find ways to ease privacy concerns. Even if they cannot, she said the need is important enough to amend the 1947 National Security Act. She suggested that this might include creation of a domestic intelligence agency, in part to address concerns about law enforcement access to intelligence on US persons.

Harding argued that US persons' privacy is a "third rail" with Congress that the IC should not touch. This implies that the IC would not delve as deeply into some topics and issues as Wood suggests it needs to cover. Barrett commented that he tended to agree with Harding. He suggested that a Consortium might offer ways to fully exploit OSINT sources while protecting privacy. Gordy noted that Janes follows EU privacy law, which restricts its ability to prepare intelligence on individual people. This suggests some limits on the ability of private firms to satisfy intelligence requirements as well as the potential that privacy concerns in other countries will lead to further restrictions, including on the availability of OSINT.

Looking Beyond OSINT

Resource Tradeoffs

As noted, Roundtable participants all agreed that more resources need to be devoted to OSINT and that it could more efficiently satisfy many intelligence requirements than other INTs. They also agreed that a top-line increase in the IC's budget is improbable. This means that money and perhaps people would need to be shifted from other INTs to successfully pursue any of the OSINT approaches. However, beyond a quip that perhaps the IC could forego building another satellite, participants did not have proposals on what resources to shift.

This was not surprising given that making tradeoffs among programs and INTs is a longstanding IC challenge. There are minimal mechanisms beyond the budget process and common sense to divvy up responsibility and resources among INTs and the IC components that pursue them. There is no way to determine how many resources of whatever type should be devoted to each topic other than its prioritization in the NIPF or similar guidance documents. And, there is no way to measure the inherent "value for money" policymakers place on satisfying each requirement.

OSINT's overlap with all the other INTs and its ability to provide insights on all NIPF topics from the lowest priority global coverage issue to the highest priority hard target suggest it may be particularly difficult to specify tradeoffs. Success implementing the IC OSINT strategy or a well-constructed Consortium pilot might eventually point to tradeoffs some topics. However, unless mechanisms to implement tradeoffs are created, it is more likely that other components would continue to cover the same topics like little kids playing soccer. At most, those components would seek to shift their resources to close gaps on other topics rather than ceding them to OSINT components.

Role and Structure of the IC

Participants' comments on the volume of PAI/CAI and the private sector's ability to exploit it suggest that resource tradeoffs may include consideration of fundamental change in the IC. The IC that has grown up since World War II is largely structured and resourced to uncover secrets clandestinely through a range of human and technical means. These were developed largely because there were no open sources or other ways to uncover the secrets. The information explosion at least raises the potential that much of what the IC does is outmoded or soon will be.

None of the speakers or other participants suggested the IC be abolished or revert to its pre-World World II scope, but several comments suggested the IC risks consumers seeing it as not providing "value for money." If so, its future might be in question. Usher commented, for example, that it would be very bad for the IC if Congress could meet its need for intelligence on Gaza by turning to Janes, while Gordy noted his firm already sells intelligence directly to several parts of the Joint Staff, bypassing the J-2.

Gordy came closest to offering a way forward in his argument that the IC should focus on niches where exquisite clandestine human and technical collection is needed while relying on the private sector to provide OSINT on everything else. He did not suggest any niches or other changes in IC structure and resources. These could vary based on such factors as the overall size of the niches, the resources needed to provide intelligence on them, and whether consumers saw getting the intelligence as worth the investment.

Peak OSINT?

A final area that bears more research and discussion is whether OSINT will continue to explode in quantity and availability. All four approaches take as a given that the quantity of information will continue to grow over the next

two decades and that the rate of expansion will even accelerate as AI tools mature. They also agree with private sector experts that it will be available to exploit as PAI or CAI.[a] Victor's article should raise some doubts, however, on both quantity and availability. China is not the only country that is improving digital security, not least by exposing less sensitive information in the first place. In July 2024, for example, Russia banned use of personal cell-phones by its military on the frontlines with Ukraine in response to press reports that indicated metadata was being used to track battles.[b]

The balance in the race between cyber defense and offense may shift, and the ability of private firms and individuals to ferret out useful intelligence may decline. The impact of privacy safeguards is another uncertainty. Legal safeguards and encryption are likely to grow in the West and perhaps spread more broadly. If safeguards expand or enough people take actions to secure their privacy, the availability and utility for intelligence of at least some types of digital data might decline.■

a. See Emily Harding, "Move Over JARVIS, Meet OSCAR," January 19, 2022. https://www.csis.org/analysis/move-over-jarvis-meet-oscar.
b. Veronika Melkozerova, "Russia Cracks Down on Personal Cell Phones on the Front Line," *Politico*, July 24, 2024. https://www.politico.eu/article/russian-duma-adopts-law-on-punishment-for-soldiers-using-gadgets-on-the-frontline/.

Endnotes

1. Link to Strategy. https://ddi.cia/odni-and-cia-release-the-intelligence-community-osintstrategy-for-2024-2026/
2. J.J. Bagnall, "The Exploitation of Russian Scientific Literature for Intelligence Purposes," Vol. 2, No. 3 (1958), declassified September 18, 1995; Davis W. Moore, Jr., "Open Sources on Soviet Military Affairs," Vol. 7, No. 2 (1963), declassified September 18, 1995; Herman L. Croom, "The Exploitation of Foreign Open Sources," Vol. 13, No 3 (1969), declassified August 25, 1997; Gail Solin, "The Art of China Watching," Vol. 19, No. 1 (1975), declassified July 2, 1996; David Gries, "Intelligence in the 1990s," Vol. 35, No. 1 (1991); David Overton, "The DI Ten Years After Reorganization," Vol. 36, No. 5 (1992); Mark Lowenthal, "The State of the Art, the Artless State," Vol. 45, No. 2 (2001); John Gannon, "The Strategic Use of Open-Source Information," Vol. 45, No. 3 (2001); Martin Petersen, "The Challenge for the Political Analyst," Vol. 47, No. 1 (2003); Stephen Mercado, "Sailing the Sea of OSINT in the Information Age," Vol. 48, No. 3 (2004); Chris Rasmussen, "How the Intelligence Community Has Held Back Open-Source Intelligence, and How it Needs to Change," Vol. 68, No. 2 (2024).