JANUARY 2025

NSI | THE NATIONAL SECURITY INSTITUTE
At George Mason University's Antonin Scalia Law School

A STANDALONE OSINT AGENCY FOR STRONGER NATIONAL SECURITY

By David Gauthier

NSI LAW AND POLICY PAPER

A STANDALONE OSINT AGENCY FOR STRONGER NATIONAL SECURITY

THIS NSI LAW AND POLICY PAPER:

1. **SUMMARIZES** the growing importance of open-source intelligence (OSINT) to national security.

2. **DESCRIBES** the current IC strategy and implementations of OSINT capabilities.

3. **ARGUES** for a standalone independent OSINT agency inside the Executive Branch to strengthen and foster OSINT as a unique information discipline.

ABOUT THE AUTHOR

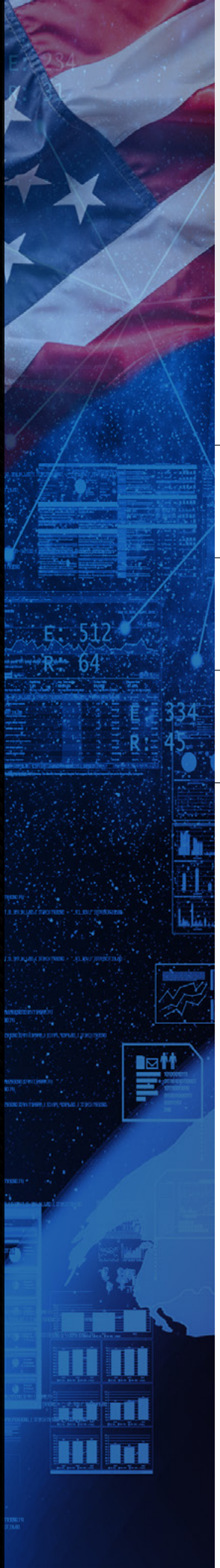
DAVID GAUTHIER

Visiting Fellow at GMU NSI & Chief Strategy Officer for GXO, Inc.

David Gauthier brings over 27 years of experience in U.S. national security as an intelligence officer, technology innovator, and strategic leader. In 2023 he became the Chief Strategy Officer of GXO, Inc., a full-service consultancy helping space industry innovators grow sustainable solutions for national security. Mr. Gauthier also serves as the Vice Chair for NOAA's Advisory Committee on Excellence in Space (ACES), is a Senior Associate (Non-Resident) with the Center for Strategic Intelligence Studies (CSIS), and a Visiting Fellow for the National Security Institute at George Mason University.

Mr. Gauthier served in the Senior Executive Service for nine years prior to his role with GXO, Inc. He was the founding Director of Commercial Operations at the National Geospatial-Intelligence Agency (NGA) and the first-ever Chair of the Intelligence Community's Commercial Space Council. Mr. Gauthier was also NGA's Chief Strategy Officer and the Portfolio Lead for Activity-Based Intelligence. Over his career he led intelligence efforts at NGA, ODNI, DIA, and the U.S. Air Force, gaining expertise in technical remote sensing, OPIR operations, all-source intelligence, national space policy, and AI.

Mr. Gauthier earned M.S. degrees in both Aerospace Engineering and Telecommunications Science from the University of Colorado at Boulder and a B.S. degree in Electrical Engineering from the Rensselaer Polytechnic Institute. He is a graduate of MIT Sloan's Executive Education, DoD's APEX, and ODNI's Leading the IC; and is the recipient of several awards including a National Intelligence Professional Award, Meritorious Civilian Service Medal, and the Presidential Rank Award.



CONTENTS

BACKGROUND

WHAT IS OPEN-SOURCE INTELLIGENCE OR OSINT?

- **Intelligence Community definition.** The recently released Intelligence Community (IC) OSINT Strategy states, "OSINT is intelligence derived exclusively from publicly or commercially available information that addresses specific intelligence priorities, requirements, or gaps."[1]
  - Generally, open-source intelligence (OSINT) can refer to a wide-range of information and sources that are free, public, and legal to access, including information obtained from the media, such as newspapers, television, and blogs, as well as from professional and academic records, and public government data – for example, government reports.
  - OSINT purposefully excludes any data that requires privileged or classified access to government systems.
- **History of OSINT in the IC.** While the IC has historically gathered OSINT from foreign publications, its primary focus before 9/11 was on acquiring classified state secrets. Since these secrets were not publicly available online, the IC placed limited value on analyzing 'open source' information. It was only in 2005 that the Office of the Director of National Intelligence (ODNI) opened the Open-Source Center (OSC) in response to the 9/11 Commission's recommendations to improve the integration of information gleaned from both open and clandestine sources.[2] Since then, the OSC has been generating unique value for intelligence reporting, and in 2015, it was moved into the Central Intelligence Agency's (CIA) Directorate of Digital Innovation as the Open-Source Enterprise.[3]
- **OSINT is separate from the traditional intelligence process.** OSINT can never replace high-value government sources and methods for collecting information, such as national technical means and counterintelligence activities. These methods are so burdensome or expensive that only nation-states typically undertake such efforts. Instead, OSINT relies on an asymmetric information advantage that is now available to private organizations due largely to the ability of artificial intelligence (AI) to digest enormous amount of openly available data.

THE INFORMATION REVOLUTION

- **Today's publicly available information.** Today's public is now privy to an unprecedented amount of data and information gleaned from open sources, often called Publicly Available Information or PAI.
  - The amount of data available in the public arena has grown exponentially due to the rapid proliferation of Internet-connected devices, global remote sensing systems, and individuals utilizing content generation services. Some estimates show that over 400 terabytes of online content are created every day.[4]

- **New creators of OSINT.** Public and private organizations can now use powerful AI tools, including off-the-shelf large language models (LLMs) like ChatGPT, to efficiently process the enormous amount of data available in the public arena. Using AI tools makes it possible for a company, organization, or even individuals external to the U.S. government (USG) or IC to easily derive critical, decision-ready information from open sources and publish meaningful OSINT products and services.
    - Information-rich professions like heath care and law generate large amounts of new open source information daily. While practitioners in these areas have struggled to stay current in their fields, they are now finding increased productivity through tools like ChatGPT.[5]
    - Top consulting and strategy companies now allow their experts to use LLMs and other AI tools to aid clients in making business decisions, ranging from investment optimization and supply chain efficiency to enhanced climate impact forecasting.[6]
    - Trained OSINT practitioners can also use their skills to overcome common limitations of these widely-available AI tools. For example, an OSINT practitioner can identify an LLM's limitations, such as limited or outdated training data, AI's ability to interpolate answers that are inaccurate or hallucinated, and then apply their craft to avoid making such mistakes.

OSINT'S GROWING GEOPOLITICAL VALUE

- **Strengthening partnerships while building international support.** Journalists and news organizations for centuries have served their profession by conducting open-source research and publishing OSINT. Russia's February 2022 invasion of Ukraine highlighted the value of unclassified and shareable information from remote sensing satellites in the hands of embedded content creators who assisted in guiding diplomacy, building coalitions, and informing public opinion.[7] OSINT published by the media and others galvanized NATO support for Ukraine and aided both defenders and humanitarian groups in their efforts to save civilian lives.[8]
- **Revealing truth and countering deception in world affairs.** OSINT enhances democratic states' abilities to obtain intelligence and freely share it with allies and the general public. For example, OSINT openly and objectively showed Russian atrocities to the global community, making them impossible to ignore.[9] When combined with lies from Russian leadership and state-sponsored media, OSINT revealed the nature of Russian deception and the manipulation of the truth to support their narrative.[10]
- **Revealing disinformation in traditional media.** Spreading disinformation through traditional media is now a common geopolitical strategy for sowing discord[11] in what has been called a "war of narratives."[12] OSINT can be used as a check and balance on traditional media, evaluating bias within media reporting where increasing polarization means that audiences are sometimes exposed to only the news they are likely to believe without the benefit of objectivity.[13]

- The Trust in Media Cooperative is a non-profit using OSINT to provide consumers with tools to empower themselves to critically assess media content. Their mission is to provide access to information quality scores derived from unbiased standards and tools. These tools aim to reveal to the consumer the biases, falsehoods, and provenance of information used by the media.[14]

- **Verifying Artificial Intelligence insights.** OSINT can also play a critical role as an independent validator of AI. An AI model must be continuously verified using unbiased and truthful information sources for it to be trusted and responsible.[15] OSINT practitioners can periodically fact-check AI answers, corroborate AI-driven storylines, and publish trends in AI model accuracy.
  - For example, if OSINT practitioners show that a publicly-available AI tool has been misidentifying activities along contested borders, they could highlight that this AI tool and its findings have been misused for geopolitical purposes.[16] These adversarial AI attacks are similar to, but far more insidious than, internet vandals changing Wikipedia pages to align with their personal ideologies or financial incentives.[17]

THE ROLE OSINT CURRENTLY PLAYS IN U.S. NATIONAL SECURITY

- **OSINT demonstrates value to national security.** OSINT already provides real value to U.S. national security interests, including delivering original insights gleaned from large amounts of geospatial data; the timely delivery of Tactical Surveillance, Reconnaissance, and Tracking (TacSRT) information to users; and the broad applicability of geospatial indications and warnings from applying data science to large, multi-source remote sensing data sets. Ongoing USG projects also highlight another key benefit of OSINT, the ability to immediately share data and products with partner nations.
  - The National Geospatial-Intelligence Agency (NGA) sponsors the Tearline Project, which leverages the research and analysis power of universities and non-profit organizations to analyze large and open data sets to increase public awareness and inform decision-makers about national security concerns. Tearline producers routinely generate original insights on national security related topics, including various strategic, economic, and humanitarian intelligence issues.[18]
  - The U.S. Space Force (USSF) has started to implement its commercial space strategy aimed at quickly "driv[ing] the development of more resilient and combat-capable architecture."[19] A key component of its strategy is the Tactical Surveillance, Reconnaissance, and Tracking (TacSRT) project. TacSRT harnesses commercial resources to meet military needs in the field and enables the USSF to rapidly purchase open-source analytic products and insights for tactical users on expedited timelines. Commercial data sources and products are also "readily releasable to partner nations enhancing the combatant command's ability to conduct security cooperation. As a result, potentially life-saving data can be delivered to combatant commands in near-real time to inform and accelerate emergency response activities."[20]

- The company Ursa Space has created a Global Monitoring Service which provides customers satellite-derived insights from across its virtual constellation of 22 satellite imagery providers, which is also fused with other open data sources in near real-time.[21] The goal of the Global Monitoring Service is to provide unclassified and shareable insights to military and coalition users.

- **IC OSINT strategy looking forward.** The new IC OSINT Strategy, published by the ODNI in March 2024, states that OSINT is "vital" to the IC's mission and must be embraced to maintain intelligence advantage.[22] This document highlights the additional value OSINT brings and that its adoption and integration into the IC is a necessary expansion of their capabilities.
  - The IC OSINT Strategy's mission lays out a vision of a "professionalized, integrated, and agile IC OSINT enterprise providing decision advantage for U.S. policymakers and warfighters and driving innovation with partners."[23]
  - To successfully meet the goals of the IC OSINT Strategy, a paradigm shift in IC-private sector collaboration is imperative. This new approach should leverage private industry's cutting-edge IT innovations and scalable computing capabilities to extract valuable insights. To accomplish this, the IC OSINT Strategy notes that "robust partnerships with industry, academia, and foreign counterparts will be essential for success."[24]

KEY ISSUES **AT STAKE**

DISPERSED AND DISJOINTED IC OSINT IMPLEMENTATION

- **IC versus the Department of Defense.** For several years, the Intelligence Community and the Department of Defense have maintained separate governance bodies for the development of their OSINT capabilities. However, now that the IC has published a new OSINT Strategy, it appears they have taken the lead in operational implementation. Nevertheless, the IC admits that it will take an immense effort to organize a "dispersed discipline with practitioners across many different components."[25]
  - The level of effort necessary to coordinate, aggregate, and integrate the many OSINT efforts undertaken by a dispersed IC risks that it will crumble under the weight of its own bureaucratic complexity.
- **Challenges of multiple IC implementations.** Greater use of OSINT inside the IC may detract from core IC mission functions, confuse intelligence consumers, and artificially increase confidence in assessments.[26] Because of these risks, implementing OSINT in the IC may be disjointed and less effective than a separate entity focused entirely on generating insights from OSINT.

SECRECY VERSUS SPEED IN PROMOTING TRUTH

- **Secret information is powerful, but fast information can be more powerful.** The disclosure of classified information significantly undermines a government's strategic position. When secrets such as advanced weapons specifications, covert intelligence collection methods, and confidential military information are exposed, nations lose both diplomatic leverage and the crucial element of surprise in military operations. For good reasons, the IC deliberately withholds knowledge of adversary capabilities and plans to ensure U.S. countermeasures maintain long-term advantage.
  - While secrecy is crucial, over-classification often creates an unwieldy bureaucratic burden, impeding the flow of information within government channels and hampering the rapid decision-making process required to compete in the information age. In situations where decision speed will determine strategic advantage, insights from OSINT may outperform traditional intelligence processes.
- **There is new power in revealing truth.** In an era of strategic competition, nations use the tools of diplomacy, information, and economics through open and transparent means to deter and shed light on adversary aggression. OSINT can be used to reveal secrets about the adversary so their aggression and deception can no longer be hidden from public view. Using OSINT to promote the truth can reinforce diplomatic and economic partnerships while simultaneously forcing adversaries to work harder to overcome their continuous information disadvantage.

AUTHOR'S **VIEWS**

OSINT BECOMES MORE POWERFUL EVERY DAY

- **Increasing digital information plus the AI tools to comprehend it**. The digital information revolution has developed so quickly that until recently it was a huge burden to distill meaningful insights at scale and to gain a competitive information advantage from them. This meant the vast resources of the USG designed to aid decision-making continued to give the IC an advantage. Within the past two years, however, the rise of generative AI tools has given private users the power to comprehend massive amounts of data and to derive complex insights in real time.[27] This shift in power across the information domain increases the value of OSINT.
- **Maintaining the USG's information advantage.** While the USG has historically relied upon its own unique classified sources to gain the upper hand in diplomatic and military arenas, the USG must now also harness the vast amounts of publicly available digital information and focus on OSINT as a new discipline or risk losing its information advantage to the "data deluge."[28]
- **OSINT is now critical for statecraft and deterrence.** In the digital age, where speed in decision-making is critical and "successful statecraft increasingly demands winning the information competition and shaping public narratives,"[29] OSINT will provide critical information advantages.

EVERY IC AGENCY NEEDS TO INTEGRATE OSINT TO STAY RELEVANT

- **OSINT adds value and context to intelligence reporting**. It is necessary for each IC agency to incorporate OSINT insights into their unique tradecraft and analytic disciplines to "augment and contextualize clandestinely acquired information."[30]
- **IC agencies must develop sub-disciplines of OSINT for themselves.** To enhance their respective missions, such as communications network analysis, geospatial/imagery analysis, or predicting foreign military capabilities, each IC agency should establish a dedicated OSINT function tailored to their specific intelligence requirements, providing another stream of information to complement their existing classified intelligence sources. These efforts should be focused on integrating external OSINT into internal agency operations.

AN INDEPENDENT OSINT AGENCY IS CRITICAL FOR NATIONAL SECURITY

- **OSINT in the IC is necessary but not sufficient.** With more data and analysis tools now available for open and private researchers, analysts, scientists, programmers, and journalists, having a dedicated function in the IC to evaluate and integrate non-government data at scale is necessary.

However, managing the totality of OSINT from inside the IC is not only insufficient for strategic competition in the information age, it will also handicap its potential.

- First, the high administrative and bureaucratic cost of managing, standardizing, and coordinating OSINT efforts across the 18 IC agencies will stifle productivity. Forcing each IC agency to adopt their own version of an OSINT function and subsequently deconflict them may become counter-productive.
- Second, only maintaining OSINT as a side-mission at each IC agency risks that it will be forever under-resourced and under-utilized given the cultural biases for classified sources. OSINT insights may even be dismissed outright whenever providing any evidence contrary to that derived from classified sources.[31]
- Third, data sources and the AI tools used to generate insights are proliferating so rapidly, it requires a dedicated organization to understand state-of-the-art information technologies, adapt AI governance, and fully embrace the ongoing information revolution outside of classified networks that were designed to protect information rather than make it interoperable.[32]

- **The USG needs a stand-alone all-source OSINT agency outside of the IC.** To derive maximum benefit from expansion of OSINT, an independent USG agency outside of the IC must be created to avoid the pitfalls of interagency governance, information bias, overclassification, and groupthink.
  - A single agency responsible for professionalizing the OSINT discipline can more efficiently develop the necessary standards, strategies, policies, regulations, tactics, techniques, and procedures than a multi-agency function inside the IC.
  - An independent OSINT agency shifts the organizational mindset from OSINT as a secondary source to being the only source, maximizing OSINT's utility to the diplomatic, intelligence, military, and economic levers of national power.
  - An agency focused on OSINT enables independent analytic conclusions drawn from different sets of data to ensure information resilience for warfighters and policymakers.
  - A standalone OSINT agency should be the primary source of verified and vetted news and information for the Executive Branch with the IC creating additive value using classified sources and methods. By optimizing the relationship between OSINT and secret intelligence, a state of productive competition can improve the performance of both.[33]
  - This stand-alone agency should avoid security clearances on principle, thereby removing the temptation to classify information and ensuring maximum information effectiveness through speed, scale, and shareability – increasing the agency's utility to the nation.[34]
- **OSINT and the National Security Council.** The new OSINT agency should have a seat on the National Security Council (NSC) to ensure its equivalency with the DNI. This will also create an atmosphere of competition between the two entities for delivering information advantage. A secondary effect may be that the IC is able to rededicate resources on truly asymmetric information gathering to derive unique insights that are completely unavailable to the OSINT community.

ACTIONABLE **RECOMMENDATIONS**

1 CREATE A DEDICATED OSINT AGENCY OUTSIDE OF THE IC

- **Create an independent Executive Branch "Open Source Information Agency" (OSIA) outside of the IC starting with existing resources.** There are already several disparate OSINT efforts that could be coalesced into a cohesive agency dedicated to informing and advising the Executive Branch with trusted information.
  - The OSIA could initially be created as a task force within the Executive Office of the President, much like the White House Office of Homeland Security in 2001[35] and the U.S. Digital Service in 2014.[36]
  - The OSIA could then be resourced by consolidating elements across the federal government with a similar mission. Some initial resources could come from the IC's Open Source Enterprise, the U.S. Digital Service, the U.S. Agency for Global Media, and the Office of the Federal Chief Information Officer. These resources, which currently support OSINT programs, would provide the new agency with the expertise needed to initiate OSINT operations. Resources would transfer from these existing organizations via an appropriations bill passed by an act of Congress.
  - A goal of re-appropriating $25 million, along with 25 government civilian personnel, from existing OSINT and similar efforts across the government would likely be sufficient to create the nucleus of a new OSIA. This would allow the agency to begin its initial establishment and operational efforts.
- **Creation of an entirely new federal agency will also require new federal resources to accomplish the mission goals set out in this paper.** Such resources would be appropriated through an act of Congress, similar to the process used to create the Office of Science, Technology, and Policy in 1976[37] and the Department of Homeland Security in 2002.[38]
  - An appropriation of an additional $75 million, in addition to 75 more government civilian personnel, would build sufficient strength to begin mission operations as a standalone OSINT agency.
  - The combination of repurposing existing OSINT capabilities and appropriating new federal resources would effectively create an OSIA with an initial capacity of $100 million and 100 civilian personnel. These resources would enable the OSIA to establish its administrative structure, initiate operations, and develop plans and programs. For reference, this is less than half the size of the U.S. Digital Service currently serving inside the Executive Office of the President.[39]
  - It is expected any future growth would then be determined by mission needs and requirements and resourced appropriately.

- **The OSIA would be responsible for evaluating, protecting, and delivering open source news, research, and information to support the decisions of the Executive Branch.** In this regard it would act as a trusted source of news, an unbiased research service, and a steward of digital information for the federal government. Specifically, the OSIA would:
  - Set standards for evaluating trust in media/information and create national policies for federal agencies' use of open source information in executing their mission;
  - Operate an enterprise dedicated to the collection, analysis, and protection of open source information;
  - Deliver timely news and information to the Executive Branch, including to the IC agencies who would then add their own unique knowledge and insights derived from classified sources and methods;
  - Detect and counter disinformation and bias in the mainstream media. This role not only helps OSIA provide trusted news and information to the federal government, it also serves free and open societies globally who are vulnerable to adversarial disinformation campaigns supercharged by AI; and
  - Provide a continuous source of truth to help government agencies monitor their critical AI models for any evidence of tampering, bias, drift, or loss in performance. For the nation to trust AI information it is necessary for a source of unbiased truth to serve as an ongoing litmus test.

2 GIVE THE NEW OPEN SOURCE INFORMATION AGENCY A SEAT ON THE NSC

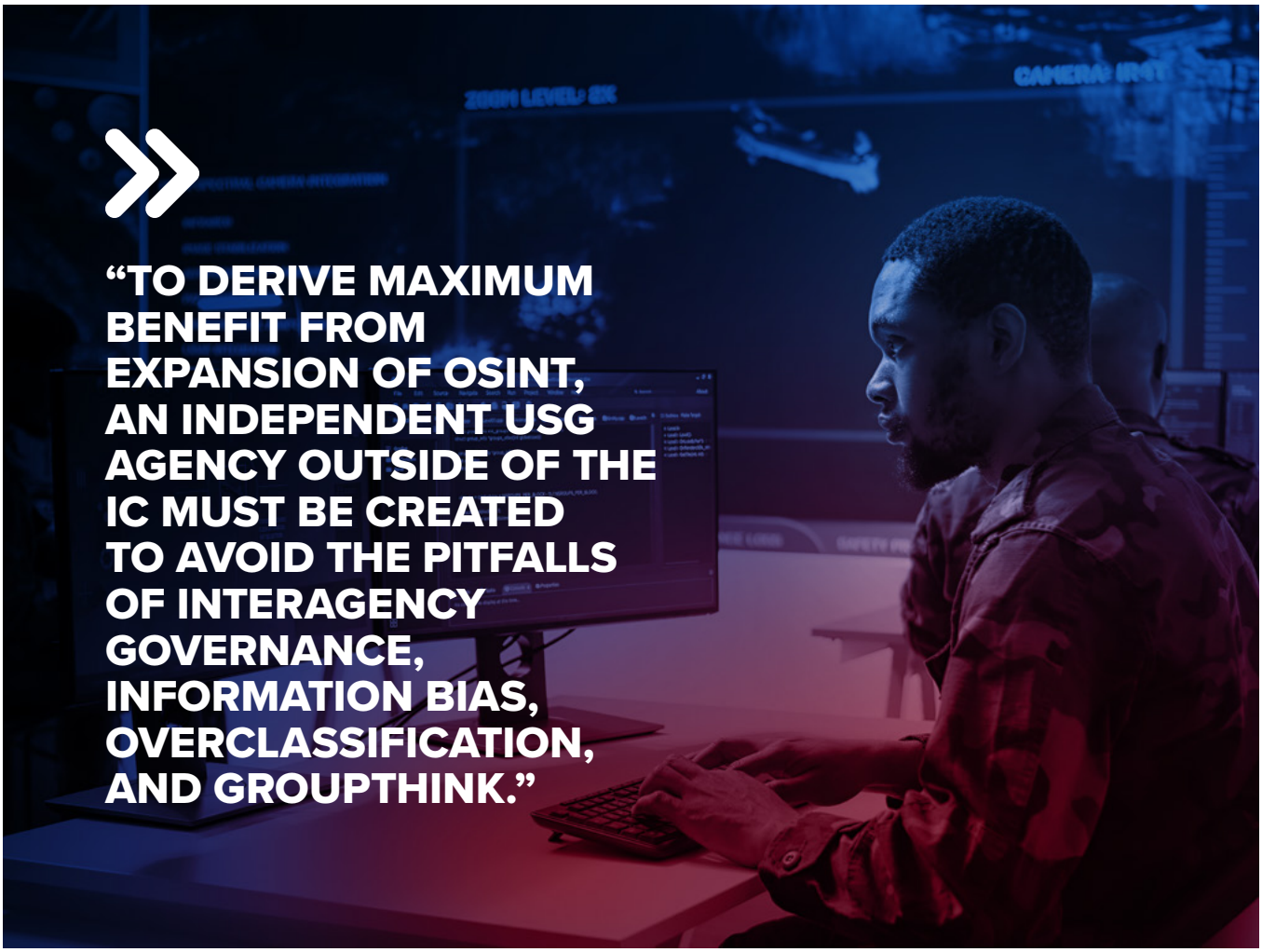
- **The OSIA should have a seat on the National Security Council (NSC) to fully harness the unique data sources, high-tech tradecraft, and deep insights OSINT can provide to decision-makers, particularly in the current era of great power competition.** This position would speak to geopolitical events through the lens of media, data, and information available in the public sphere and would coordinate closely with the DNI on any adversarial attempts to control narratives and spread disinformation to specific populations.

3 EXPAND THE OSINT DEFINITION

- To ensure relevance across the entire federal government, the definition of OSINT should be expanded to include the analysis of openly available data and information from multiple sources including public, commercial, and sometimes private domains when offered freely to the USG.
  - OSINT should include the "deep web" or "dark web" because even though this information does not appear in search engines, it is still publicly available.[40]
  - OSINT should also include private information that is volunteered or from sources in the unclassified domain. Some examples of this include advertising data, shipping/trade records, private weather/climate data records, and insurance analyses typically owned by a single company or entity.

4 MAINTAIN OSINT INTEGRATION ACTIVITIES INSIDE EACH IC AGENCY

- **Each IC agency should create and maintain a dedicated OSINT element to facilitate information flow from the OSIA to inform and augment classified analysis.**
  - The IC should develop additional clandestine collection sources and methods that will serve to improve, confirm, or deny the information gleaned from OSIA.
  - Each IC element responsible for OSINT awareness would report to that agency's head of analysis.
  - The IC should develop and implement a lightweight governance structure across the IC, such as a council of OSINT element leads, which would ensure there is a level of inter-agency coordination and standardization in how OSINT is handled amongst IC agencies.



ENDNOTES

1 Office of the Director of National Intelligence, The IC OSINT Strategy 2024-2026 (2024), https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf.

2 "Press Release, Office of the Director of National intelligence, ODNI Announces Establishment of Open Source Center (Nov. 8, 2005), https://www.dni.gov/files/documents/Newsroom/Press%20Releases/2005%20Press%20Releases/20051108_release_content.htm.

3 *Open Source Enterprise*, Wikipedia (Feb. 29, 2024), https://en.wikipedia.org/wiki/Open_Source_Enterprise.

4 Fernando Duarte, Amount of Data Created Daily (2024), Exploding Topics (July 3, 2024), https://explodingtopics.com/blog/data-generated-per-day.

5 Martin Neil Bailey & Aiden T. Kane, "How Will AI Affect Productivity?", Brookings (May 2, 2024), https://www.brookings.edu/articles/how-will-ai-affect-productivity/.

6 Press Release, Bain & Co., Bain & Company Announces Services Alliance with OpenAI to Help Enterprise Clients Identify and Realize the Full Potential and Maximum Value of AI (2023), https://www.bain.com/about/media-center/press-releases/2023/bain--company-announces-services-alliance-with-openai-to-help-enterprise-clients-identify-and-realize-the-full-potential-and-maximum-value-of-ai/; see also Som Biswas, Importance of ChatGPT in Agriculture: According to ChatGPT (Mar. 30, 2023), https://ssrn.com/abstract=4405391.

7 T.X. Hammes, Game-Changers: Implications of the Russo-Ukraine War for the Future of Ground Warfare, Atlantic Council (2023), https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/game-changers-implications-of-the-russo-ukraine-war-for-the-future-of-ground-warfare/.

8 Press Release, EOS Data Analytics, EOS Data Analytics Urges Satellite Imagery Firms and Space Agencies to Stand with Ukraine (Mar. 2, 2022), https://www.prnewswire.com/news-releases/eos-data-analytics-urges-satellite-imagery-firms-and-space-agencies-to-stand-with-ukraine-301492357.html.

9 Deborah Amos, Open Source Intelligence Methods Are Being Used to Investigate War Crimes in Ukraine, *NPR* (June 12, 2022), https://www.npr.org/2022/06/12/1104460678/open-source-intelligence-methods-are-being-used-to-investigate-war-crimes-in-ukr.

10 Catherine Belton, Kremlin Runs Covert Disinformation Campaign to Undermine Zelensky, *Washington Post* (Feb. 16, 2024), https://www.washingtonpost.com/world/2024/02/16/russian-disinformation-zelensky-zaluzhny/.

11 Juan Soto, The Disinformation War, American Security Project (Oct. 6, 2020), https://www.americansecurityproject.org/disinfo-wars/.

12 Elena Davlikanova et al., The War of Narratives: The Image of Ukraine in Western, Russian and Ukrainian Media (1991-2022), ResearchGate (July 2023), https://www.researchgate.net/publication/371981848_The_War_of_Narratives_The_Image_of_Ukraine_in_Western_Russian_and_Ukrainian_Media_1991-2022.

13 Luke Auburn, Study of Headlines Shows Media Bias Is Growing, U. Rochester News Ctr. (July 13, 2023), https://www.rochester.edu/newscenter/study-of-headlines-shows-media-bias-growing-563502/.

14 Trust in Media (TIM) Cooperative., https://www.timcoop.org/.

15 National Telecommunications and Information Administration (NTIA)., AI Accountability Policy Report (2024), https://www.ntia.gov/issues/artificial-intelligence/ai-accountability-policy-report.

16 Michael Hannecke, Adversarial Attacks in Generative AI, *Medium* (Nov. 14, 2023), https://medium.com/bluetuple-ai/adversarial-attacks-in-generative-ai-1f08f01e740f.

17 Joe Pinsker, The Covert World of People Trying to Edit Wikipedia—for Pay, *The Atlantic* (Aug. 12, 2015), https://www.theatlantic.com/business/archive/2015/08/wikipedia-editors-for-pay/393926/.

18 Tearline, https://www.tearline.mil/about-tearline/.

19 Secretary of the Air Force Public Affairs, USSF Releases Commercial Space Strategy to Increase Competitive Advantage, U.S. Space Force (Apr. 10, 2024), https://www.spaceforce.mil/News/Article-Display/Article/3736616/ussf-releases-commercial-space-strategy-to-increase-competitive-advantage/.

20 Lisa Sodders, Space Force Leverages Commercial Data Analytics to Aid Combatant Commands in New Ways, U.S. Space Force (May 29, 2024), https://www.spaceforce.mil/News/Article-Display/Article/3793014/space-force-leverages-commercial-data-analytics-to-aid-combatant-commands-in-ne/.

21 Grey Platform (May 2, 2024), https://ursaspace.com/blog/quiet-professionals-partnership/.

22 Office of the Director of National Intelligence, The IC OSINT Strategy 2024-2026 (2024), https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf.

23 *Id.*

24 *Id.*

25 Justin Doubleday, Intel Agencies Just "Scratching the Surface" on Open Source Initiatives, Federal News Network (Aug. 14, 2023), https://federalnewsnetwork.com/intelligence-community/2023/08/intel-agencies-just-scratching-the-surface-on-open-source-initiatives/.

26 George Wilde, The IC's Biggest Open-Source Intelligence Challenge: Mission Creep, *Just Security* (Feb. 3, 2023), https://www.justsecurity.org/84997/the-ics-biggest-open-source-intelligence-challenge-mission-creep/.

27 Daniel Newman, What to Know About Where ChatGPT Is Going in 2024, *Forbes* (Dec. 18, 2023), https://www.forbes.com/sites/danielnewman/2023/12/12/what-to-know-about-where-chatgpt-is-going-in-2024/?sh=baef48d689dc.

28 Sandra Erwin, Geospatial Intelligence Gets Smart, *SpaceNews* (May 7, 2024), https://spacenews.com/geospatial-intelligence-gets-smart/. See also Peter Martin & Katrina Manson, Open-Source Intelligence Challenges CIA, NSA, Spy Agencies, *Bloomberg* (Jan. 29, 2024), https://www.bloomberg.com/news/newsletters/2024-01-29/open-source-intelligence-challenges-cia-nsa-spy-agencies.

29 Ben Scott, Why the U.S. Intelligence Community Needs an OSINT Agency, Lawfare (May 1, 2024), https://www.lawfaremedia.org/article/why-the-u.s.-intelligence-community-needs-an-osint-agency.

30 Gavin Wilde, The IC's Biggest Open-Source Intelligence Challenge: Mission Creep, *Just Security* (Feb. 3, 2023), https://www.justsecurity.org/84997/the-ics-biggest-open-source-intelligence-challenge-mission-creep/.
31 Doubleday, Intel Agencies Just "Scratching the Surface", supra note 25.

32 Emily Harding, The IC's New OSINT Strategy Gets the Basics Right, Center for Strategic & International Studies (Apr. 2, 2024), https://www.csis.org/analysis/ics-new-osint-strategy-gets-basics-right.

33 Scott, supra note 29.

34 Chris Rasmussen, Avoiding the Secrecy Trap in Open Source Intelligence, *The Cipher Brief* (Mar. 21, 2023), https://www.thecipherbrief.com/column_article/avoiding-the-secrecy-trap-in-open-source-intelligence.

35 Department of Homeland Security, The Department of Homeland Security, National Archives & Records Administration, https://georgewbush-whitehouse.archives.gov/deptofhomeland/sect1.html (last visited Oct. 14, 2024).

36 Office of Management & Budget, 10 Years of the U.S. Digital Service: Transforming Government for the Digital Age, White House (Aug. 14, 2024), https://www.whitehouse.gov/omb/briefing-room/2024/08/13/10-years-of-the-u-s-digital-service-transforming-government-for-the-digital-age/.

37 National Science and Technology Policy, Organization, and Priorities Act of 1976, H.R. 10230, 94th Cong. (1976), https://www.congress.gov/bill/94th-congress/house-bill/10230 (last visited Oct. 15, 2024).

38 Department of Homeland Security, supra note 34.

39 U.S. Digital Service, USDS by the Numbers, https://www.usds.gov/impact-report/2024/by-the-numbers/ (last visited Sept. 19, 2024).

40 Recorded Future, What is Open Source Intelligence (OSINT) (W/ use cases). What Is Open Source Intelligence (OSINT) (w/ Use Cases), https://www.recordedfuture.com/blog/open-source-intelligence-definition.

NSI | THE NATIONAL SECURITY INSTITUTE
At George Mason University's Antonin Scalia Law School

THE NATIONAL SECURITY INSTITUTE
Antonin Scalia Law School | George Mason University
3301 Fairfax Dr., Arlington, VA 22201 | 703-993-5620

NATIONALSECURITY.GMU.EDU