APRIL 2024

INTELLIGENCE INNOVATION

REPOSITIONING FOR FUTURE TECHNOLOGY COMPETITION

SPECIAL COMPETITIVE STUDIES PROJECT

The Special Competitive Studies Project is a bipartisan, non-profit project with a clear mission: to make recommendations to strengthen America's long-term competitiveness where artificial intelligence (AI) and other emerging technologies are reshaping our national security, economy, and society.

This second Intelligence Interim Panel Report (IPR) reflects the work that the Special Competitive Studies Project (SCSP) Intelligence Panel has conducted over the past year and a half. It builds off of the first Intelligence IPR, Intelligence in an Age of Data-Driven Competition, that was summarized in our Mid-Decade Challenges to National Competitiveness report.

SCSP Leadership

Authors

William Usher
Senior Director

Katherine Kurata
Director

Meaghan Waff
Associate Director

Tara McLaughlin
Associate Director

Ylber Bajraktari
Senior Policy Advisor

Michael Mederios
Research Assistant

Elijah Boles
Research Assistant

Capt Landon Wike, USAF
Research Assistant

Senior Advisors

This report reflects the detailed, thorough work of the SCSP Intelligence Panel staff and several outside advisors. We would like to express a special note of gratitude to the late Lieutenant General (USMC, Ret.) Vince Stewart who served as an advisor to SCSP's Intelligence Panel until his passing in April of 2023. We miss his wise counsel. Lastly, we are grateful to Peter Mattis, Kristin Wood, Dawn Meyerriecks, Aram Gavoor, and Lieutenant General, USAF (Ret.) Veralinn "Dash" Jamieson who contributed portions of the text.

Table of Contents

Executive Summary

As the geostrategic rivalry between the United States and the People's Republic of China (PRC) intensifies, the nexus between technological innovation and intelligence advantage is clearer than ever. We have entered a new era defined by exploding volumes of data – much of it openly or commercially available – rapid advancements in new tools such as artificial intelligence (AI) capable of deriving insight from all this information, and an evolving innovation ecosystem in which industry and private institutions hold the advantage over governments. The United States Intelligence Community (IC) must urgently adapt to this new environment if it is to successfully navigate the challenges ahead and sustain America's competitive edge. Building on SCSP's prior recommendations, this report argues that the U.S. Intelligence Community should focus on four priorities:

- First, rapidly **scale the use of cutting-edge generative artificial intelligence (GenAI) capabilities across the intelligence cycle** to reinvent how intelligence is collected, analyzed, produced, disseminated, and evaluated. Adapting foundation models with IC data can automate discovery and analysis.

- Second, **reimagine intelligence partnerships, both domestically and abroad**. The outdated hub-and-spoke model should shift to networked alliances to harness innovation. New inroads to domestic talent, tools, and technology are also essential.

- Third, **accelerate the IC's use of openly- and commercially-available data** by creating a new public-private partnership to harness the capabilities being developed outside the U.S. Government while working to establish a dedicated Open Source entity.

- Fourth, **extend IC support to enable strategic communications**. With the right expertise, tools, and private sector links, the IC can mount agile responses and support broader government messaging across the contested digital information domain.

With urgent transformation across partnerships, communications, adoption, and access, the Intelligence Community can leverage extraordinary innovations in data and technology to sustain decision advantage amidst intensifying rivalry. The imperative is clear – the IC must adapt to navigate the future.

Imperatives and Opportunities for Change

TRADITIONAL CATALYSTS FOR TRANSFORMATION

The National Security Act of 1947 laid the foundation for the modern U.S. intelligence Community. The need to coordinate operations abroad and evaluate intelligence for the president led to the creation of the Central Intelligence Agency (CIA).[1] At the time, the dominant view was that a streamlined intelligence network headed by a Director of Central Intelligence would ensure effective intelligence support to the newly established National Security Council (NSC) structure. However, in the decades following, those original IC structures evolved around the various intelligence disciplines – the so-called "INTs." In 1952, the National Security Agency (NSA) was stood up to elevate, equip, and unify a national cryptologic and foreign SIGINT effort.[2] The National Reconnaissance Office (NRO) was established in 1961 to coordinate the U.S. Air Force and CIA's – and later the Navy and NSA's – aerospace reconnaissance activities.[3] The Defense Intelligence Agency (DIA) was created in 1961 to unify HUMINT and military intelligence capabilities more broadly to support combat-related missions.[4] Imagery, mapping and other GEOINT activities were consolidated in 1996 under the National Imagery and Mapping Agency (NIMA)[5] – now the National Geospatial Intelligence Agency (NGA).[6]

As these shifts illustrate, advancements in technology over time created imperatives for establishment of new or significant restructuring of existing institutions to keep pace with a fast-changing threat landscape.[7] Technological advances never led to wholesale transformation of the U.S. Intelligence Community. However, these incremental institutional changes may no longer be suitable nor sufficient for this moment of technological transformation, which also happens to be the epicenter of an intensifying geopolitical competition. The IC, the U.S. Government it serves, and the society it safeguards are grappling with a rapidly evolving world and an array of

[1] 50 U.S.C. § 3035. See also Pub. L. 80-253, National Security Act of 1947 § 102.

[2] Communications Intelligence, National Security Council Intelligence Directive 9 (1952); Signals Intelligence, National Security Council Intelligence Directive 6 (1972); 50 U.S.C. § 3601-3618.

[3] The NRO's existence was classified from 1961 until 1992. The official "Declassification of the Fact of Existence of the National Reconnaissance Office" took place on September 18, 1992, in a "Memorandum for Correspondents" released by the Office of the Secretary of Defense. See more at Jeffrey Richelson, Out of the Black: The Declassification of the NRO, National Security Archive Electronic Briefing Book No. 257 (2008).

[4] DoD Directive 5105.21, Defense Intelligence Agency (DIA), U.S. Department of Defense (1961). See also DoD Directive 5105.21, Defense Intelligence Agency (DIA), U.S. Department of Defense (2023).

[5] At the time, NIMA combined the following organizations: Defense Mapping Agency (DMA), CIA's National Photographic Interpretation Center (NPIC), Central Imagery Office (CIO), National Reconnaissance Office (NRO) Imagery Processing, Defense Airborne Reconnaissance Office (DARO), Defense Intelligence Agency's (DIA) Photographic Interpretation Section (DIA/PGX), Defense Dissemination Program Office (DDPO) and CIA's imagery-related elements/programs. Pub. L. 104-201, National Defense Authorization Act for Fiscal Year 1997 (1996).

[6] NIMA was renamed NGA in 2003. Pub. L. 108-136, National Defense Authorization Act for Fiscal Year 2004, § 921 (2003).

[7] Amy B. Zegart, Flawed by Design: The Evolution of the CIA, JCS, and NCS, Stanford University Press (1999).

technologies that are advancing at an unprecedented pace, exceeding that of a mere quarter-century ago.

Today, global commodity prices can drop suddenly due to computer glitches,[8] social media can amplify false or misleading information and sow political division,[9] and large corporations can fail quickly.[10] In facing this world, the U.S. Intelligence Community risks surprise, intelligence failure, and even an attrition of its importance in the absence of significant changes. In other words, U.S. intelligence is at a historic inflection point – a time when it must fundamentally transform or risk a serious decline in its relevance.[11]

To create meaningful change in the Intelligence Community, four key factors have been historically observed as drivers of change: (1) a major intelligence failure, (2) a foreign policy crisis, (3) Congressional pressure, or (4) new leadership within the White House or the IC. Linking proposed changes to one of these four dynamics increases the likelihood of successful adoption.

1. **Intelligence Failure.** A significant intelligence failure often catalyzes change within the IC. When a major event occurs, such as the 9/11 attacks, it often leads to an investigation and a critical examination of the IC's methods, capabilities, and effectiveness. This examination can lead to reforms, including changes to organizational structure, resource allocation, and information-sharing practices. For example, major intelligence failures spurred the creation of the Director of National Intelligence (DNI) position in 2004, as well as the establishment of the National Counterterrorism Center (NCTC) in 2005.[12]

2. **Foreign Policy Crisis.** A foreign policy crisis can also drive change within the IC. For example, a crisis in a particular region or country may lead to increased focus and investment in intelligence collection and analysis in that area. For example, after India and Pakistan successfully tested five nuclear devices in 1998, the Jeremiah Commission recommended several reforms to the IC to increase its focus on WMD-related topics and promote better information sharing between IC agencies.[13]

---

[8] Andrei Kirilenko, et al., The Flash Crash: The Impact of High-Frequency Trading on an Electronic Market, U.S. Commodity Futures Trading Commission (2014); Joe Rennison, N.Y.S.E. Glitch Leads to Wild Swings in Share Prices, New York Times (2023).
[9] Timothy McLaughlin, How China Weaponized the Press, The Atlantic (2021); Ed Pilkington, Anthony Weiner Resigns over Twitter Photo Scandal, The Guardian (2011); Jon Ronson, How One Stupid Tweet Blew Up Justine Sacco's Life, New York Times (2015).
[10] Andrew Toft, The Ten Biggest Energy Company Failures, Oilprice.com (2014).
[11] Michael Dempsey, On Inflection Points (2020); Andrew Grove, Only the Paranoid Survive: How to Exploit the Crisis Points that Challenge Every Company and Career, Doubleday at 3-6 (1996).
[12] The 9/11 Commission Report, National Commission on Terrorist Attacks Upon the United States (2004). The Director of National Intelligence and National Counterterrorism Center were both created through the Intelligence Reform and Terrorism Prevention Act. See Pub. L. 108-458, Intelligence Reform and Terrorism Prevention Act of 2004 (2004).
[13] Report to the President, Commission of the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (2005).

3. **Congressional Pressure.** Through its oversight and budgetary powers, Congress wields substantial influence over the IC. By holding investigations and hearings, Congress exposes IC deficiencies, prompting vital reforms. One prominent example is the Church Committee hearings in the 1970s,[14] which revealed abuses by intelligence agencies and led to the establishment of permanent oversight committees. Furthermore, Congress can enact legislation mandating changes in IC practices or structures. The Intelligence Reform and Terrorism Prevention Act of 2004, for instance, created the DNI position and the NCTC.[15] The budget cycle is integral to this process, as it provides Congress with the opportunity to shape the IC's priorities and resource allocation.

4. **New Leadership in The White House or Intelligence Community.** Changes in leadership can also lead to changes in the IC. When a new President is elected, they may bring in a new DNI or other key IC leaders who have different priorities and perspectives. Additionally, changes in leadership within the IC itself can lead to reforms, as new leaders may have different ideas about how to best organize and operate the IC. When John Brennan became Director of CIA, he launched a major reorganization that created a new Directorate of Digital Innovation and created new mission centers that integrated the Agency's operational and analytic capabilities.[16] In 2017, under the leadership of Director Mike Pompeo, CIA established two new mission centers, the Iran Mission Center and the Korea Mission Center, in order to focus resources on countering the specific threats emanating from those regions.[17] More recently, CIA Director William J. Burns restructured the agency to address the dual challenges of great power rivalry and rapid technological advancements.[18] He stood up a new CIA mission center to focus on China.

Technology As the New Catalyst

Technology has always informed the intelligence disciplines and processes. Today, however, the speed of technological transformation far exceeds that of any past era. Since the 1950s, computing power has increased in line with Moore's Law, doubling roughly every 20 months. Since 2010, this exponential growth has sped to a doubling time of just about six months.[19] Although

[14] Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, U.S. Senate (last accessed 2024).
[15] Pub. L. 108-458, Intelligence Reform and Terrorism Prevention Act of 2004 (2004).
[16] Shane Harris, CIA Director Announces Major Reorganization of Spy Agency, CBS News (2015).
[17] CIA Creates a New Mission Center to Counter China, Washington Post (2021); Shane Harris, CIA Creates a New Mission Center to Turn Up Heat on Iran, Wall Street Journal (2017)
[18] CIA Makes Changes to Adapt to Future Challenges, Central Intelligence Agency (2021); William J. Burns, Transforming the CIA for an Age of Competition, Foreign Affairs (2024).
[19] Max Roser, The Brief History of Artificial Intelligence: The World Has Changed Fast – What Might Be Next?, Our World in Data (2022).

Moore's Law may end, the application of this computing power enabled by artificial intelligence (AI) will make possible rapid advances in other emerging technologies.

Despite the limits posed by a potential end to Moore's Law, innovation in the AI industry abounds. In 2022, private investment in AI was eighteen times greater than what it was just nine years earlier.[20] This remarkable growth trajectory is exemplified by the evolution of OpenAI's GPT-3, introduced in 2020, and its more advanced successor, GPT-4, released in March 2023. These models have undergone a staggering evolution – leading to AI systems possessing language and image recognition capabilities comparable to humans, even when trained on limited or missing data.[21] As their size increases, new models are also being released at greater speed. In February 2024, Google released its newest update to Bard, its competitor to GPT, now called Gemini.[22] Later that month, OpenAI unveiled its latest model – Sora – which can create photorealistic video from text instruction.[23] The IC's 2024 Annual Threat Assessment illuminates the importance of these developments, suggesting that the convergence of emerging technologies could lead to research breakthroughs in biotechnology and other fields demonstrating the capability of integrated AI research to drive innovation beyond the scope of narrowly focused scientific inquiries.[24]

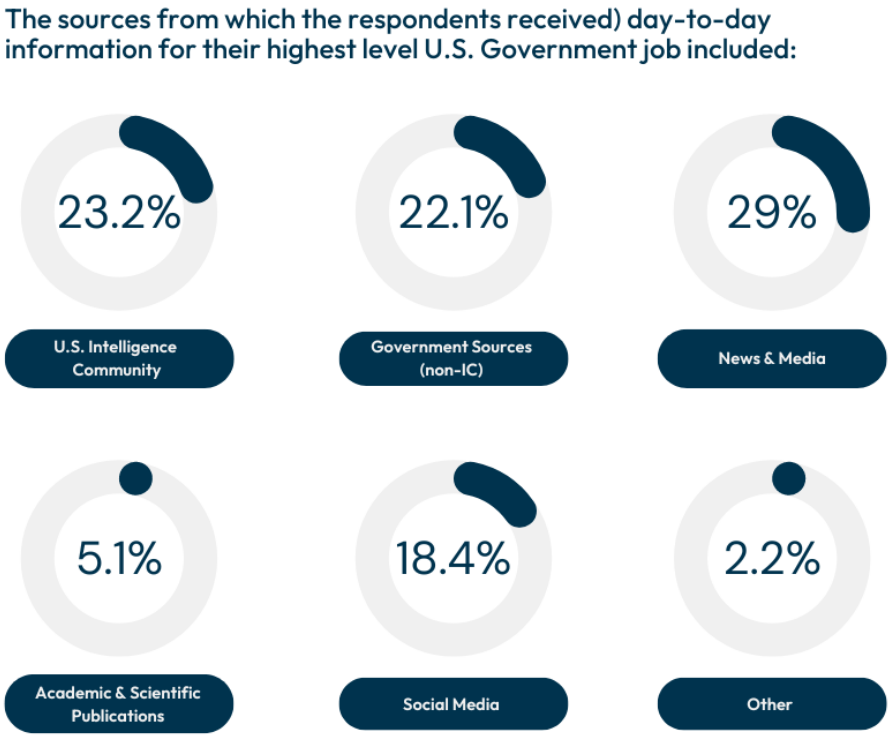
Technology is central to a set of change imperatives that include an explosive growth in data and escalating geopolitical competition with near-peer competitors, which highlights the urgency for the IC to transform itself.

Volume, Variety, and Value of Data. Across the world, the proliferation and pervasiveness of sensors has precipitated an explosion of data that has eclipsed the ability of any intelligence community to keep pace. The roughly 6.7 billion smartphone users,[25] 5.4 billion Internet users,[26] and approximately 8,500 active satellites in orbit in late 2023,[27] as well as countless applications, surveillance cameras, and sensors were expected to create 120 petabytes in 2023 and over 180 zettabytes by 2025.[28] As much as 90 percent of this data will be unstructured,[29] giving advantage to actors who are able to field AI-enabled tools to discern its veracity and value. The IC does not and need not track all this data, but it is important that it has the capability to discover insights

[20] Daniel Zhang, et al., Artificial Intelligence Index Report 2023, AI Index Steering Committee, Stanford Institute for Human-Centered AI at 171 (2023).
[21] Douwe Kiela, et al., Dynabench: Rethinking Benchmarking in NLP, arXiv (2021).
[22] Sissie Hsiao, Bard Becomes Gemini, Google Blogs (2024).
[23] David Nield, What is OpenAI's Sora? The Text-to-Video Tool Explained and When You Might Be Able to Use It, Tech Radar (2024).
[24] Annual Threat Assessment, U.S. Office of the Director of National Intelligence at 30 (2024).
[25] Petroc Taylor, Number of Smartphone Mobile Network Subscriptions Worldwide from 2016 to 2022, With Forecasts from 2023 to 2028, Statista (2023). See also Measuring Digital Development: Facts and Figures 2023, International Telecommunications Union (2023).
[26] Global Offline Population Steadily Declines to 2.6 Billion People in 2023, International Telecommunications Union (2022).
[27] Jamie Green, Befouling the Final Frontier, New York Times Magazine (2023).
[28] Petroc Taylor, Amount of Data Created, Consumed, and Stored 2010-2020, With Forecasts to 2025, Statistica (2023).
[29] Dwight Davis, AI Unleashes the Power of Unstructured Data, CIO (2019).

within these vast haystacks of information. Moreover, safeguarding access to this data is crucial to circumvent a "data trap", as emphasized by MI6 chief Richard Moore, who explicitly warned: "If you allow another country to gain access to really critical data about your society, over time that will erode your sovereignty, you no longer have control over that data."[30]

The exponential growth of digital data creates opportunities and challenges for intelligence agencies. During the Cold War, the IC monopolized clandestine information about closed adversaries. Today, many open source intelligence (OSINT) assessments from media and think tanks sources rival what the IC is able to produce using mostly classified information. However, open source has long been valued – former CIA Directors estimated 80 percent of intelligence comes from public sources.[31] Likewise, policymakers have come to rely on OSINT. In a survey conducted by SCSP in 2023, 52 percent of respondents used open sources for daily information needs and 66 percent reported using them for breaking news.[32]



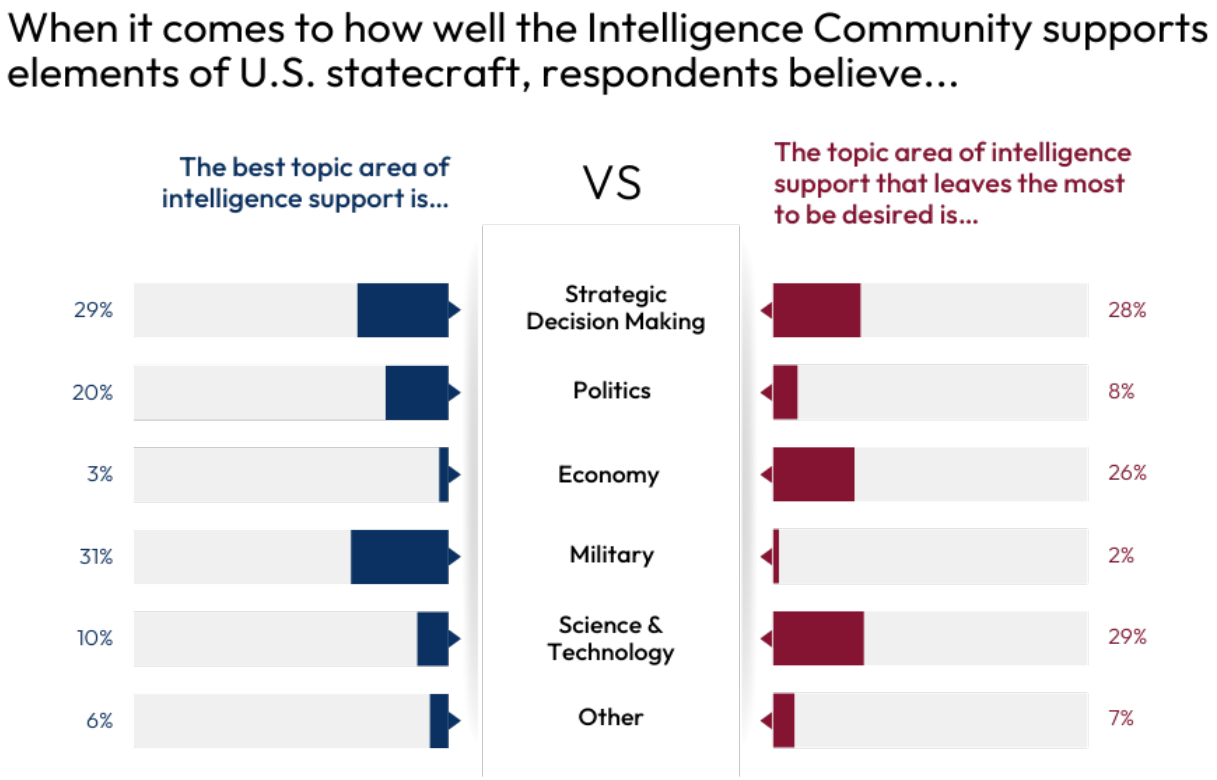
[30] George Bowden, MI6 Boss Warns of China 'Debt Traps and Data Traps', BBC (2021).
[31] Roger Hilsman, Strategic Intelligence and National Decisions, The Free Press, (1956); Lindy Kyzer, Intel Community Needs an OSINT Revolution, Clearance Jobs (2022); William Studeman, Teaching the Giant to Dance: Contradictions and Opportunities in Open Source Within the Intelligence Community, Remarks at the International Symposium on Open Source Solutions as published by the Federation of American Scientists (1992).
[32] Katherine Kurata & Ylber Bajraktari, How Can the Intelligence Community Remain Indispensable to U.S. Policy Makers?, The Cipher Brief (2023).

Amidst this data deluge, the IC must maintain unique value by collecting relevant open source data and building tools to extract insights. The IC must demonstrate continued ability to generate distinctive, actionable intelligence by skillfully blending open and classified sources. OSINT is a force multiplier, but classified sources remain vital to inform decisions and discern truth. By leveraging both, the IC can overcome today's data challenges and maintain its competitive edge.

Intensification of Global Competition. For the first time since the Cold War, the United States faces a rival – the PRC – that is competing globally across the economic, political, social, information, and military domains to reshape, if not dominate, the international order. The 2022 National Security Strategy and the 2023 National Intelligence Strategy highlight that the PRC is the only U.S. competitor with both the intent to reshape the international order and the economic, diplomatic, military, and technological power to do so.[33] Last year the Director of the FBI publicly called the PRC the "defining threat of this generation."[34] At the same time, the democratization of data and commercial tools have also empowered smaller states and non-state actors, necessitating greater intelligence efforts against a wider range of targets. The future of U.S. leadership will hinge on how well Washington can rally the world to address transnational challenges from climate change and global health to food security and economic growth, according to senior White House officials.[35]

For the IC, this intensifying technology-driven competition will shape priorities. Gaining insights into emerging innovations and the organizations that field them is now as vital as monitoring traditional political and military dynamics. While policymakers report satisfaction with IC support on political and military matters, gaps remain in other strategic areas. When surveyed, only 3 percent of policymakers saw economic issues as a leading source of IC strength, while 26 percent identified it as needing clear improvement.[36] Similarly, only 10 percent viewed science and technology as the best supported topic, while 29 percent saw it needing major improvement.[37]

[33] National Security Strategy of the United States of America, The White House at 23 (2022); 2023 National Intelligence Strategy, U.S. Office of the Director of National Intelligence at 5 (2023).
[34] More from the "Five Eyes" Intelligence Chiefs' Warning to 60 Minutes, CBS (2023).
[35] Jake Sullivan, The Sources of American Power: A Foreign Policy for a Changed World, Foreign Affairs (2023).
[36] Katherine Kurata & Ylber Bajraktari, How Can the Intelligence Community Remain Indispensable to U.S. Policy Makers?, The Cipher Brief (2023).
[37] Katherine Kurata & Ylber Bajraktari, How Can the Intelligence Community Remain Indispensable to U.S. Policy Makers?, The Cipher Brief (2023).



Organizing Principles

While continuing to cultivate its unique classified sources and methods, the IC should aim to provide more information and insight to a broader range of customers across an even wider set of issues. This larger mission is urgently needed to serve the country's needs in the future, but will only be possible if the IC leverages the power of AI and other digital tools and harnesses the growing body of openly available information. The key pillars of the IC's transformation ought to be:

Broaden Focus from "National Security" to "National Competitiveness." The new era of geopolitical and techno-economic rivalry is broadening the scope of what constitutes national security. Where conflicts once centered around conventional military capabilities, U.S. adversaries have become savvy users of hybrid warfare and new technology in attempts to exploit U.S. vulnerabilities, deter Washington from acting, and erode Western democracies' efforts to project power.[38] From cyber-attacks on major U.S. corporations like Sony Pictures,[39] Equifax,[40] and Colonial Pipeline,[41] to the use of carefully calibrated strategic messaging by the

[38] Disinformation as a National Security Issue: Former NSA General Counsel Glenn Gerstell, Intelligence Matters at 12:55 (2020).
[39] Joseph Marks, The Cybersecurity 202: The Sony Hack Ushered in a Dangerous Era in Cyberspace, Washington Post (2019).
[40] Tara Siegel Bernard, et al., Equifax Says Cyberattack May Have Affected 143 Million in the US, New York Times (2017).
[41] Colonial Pipeline Cyber Incident, U.S. Department of Energy (2021).

Kremlin during election cycles,[42] to the anti-satellite weapons being developed by countries like the PRC,[43] U.S. adversaries are leveraging technology to inflict or threaten damage on America's economy, infrastructure, and society.

Focus on Providing "Insight" over "Intelligence." Secrecy often is a necessary part of the intelligence process, particularly as a tool for protecting sources and methods as well as to buy time for U.S. decision makers to take advantage of intelligence. Yet, publicly or commercially-available data sets and AI-enabled systems are creating opportunities for far greater and faster awareness among decision makers.[44] Today, decision makers are able to have real-time insights into a wide range of issues without having to rely on classified intelligence products that could take weeks or even months to be completed. This means that the IC must balance the need for speed against the need for secrecy in order to remain effective and relevant in the modern era. By taking a risk-based approach to information sharing and investing in new tools and technologies, the IC can provide decision makers with the real-time insights they need to make informed decisions, while still protecting sensitive sources and methods.

"Lean In" on Digital Transformation. Where intelligence efforts were once the sole province of human expertise, AI now enables a fundamental shift to human-machine teaming. Emerging AI technologies like machine learning (ML) and natural language processing (NLP) already match or exceed human capabilities in selected domains. Commercial platforms that seamlessly integrate thousands of disparate data sources to provide customers with a real-time picture of business threats and opportunities already exist and offer a glimpse into the future. This integration epitomizes a transition in which AI systems transcend their roles as tools for narrow applications to active "teammates" – collaborating with humans to maximize respective strengths and uncover insights and results unreachable by either alone.[45]

[42] GEC Special Report: August 2020 Pillars of Russia's Disinformation and Propaganda Ecosystem, U.S. Department of State at 5, 14, 33 (2020).
[43] 2024 Annual Threat Assessment, U.S. Office of the Director of National Intelligence at 30 (2022).
[44] Dustin Volz, Vast Troves of Classified Info Undermine National Security, Spy Chief Says, Wall Street Journal (2022).
[45] James Wilson & Paul R. Daugherty, Collaborative Intelligence: Humans and AI Are Joining Forces, Harvard Business Review (2018).

Seizing the AI Moment for Intelligence Advantage

Recent rapid advancements in AI have made it clear that we are on the threshold of the next era of intelligence, one that will be defined by how well intelligence services leverage AI tools to collect, sift, and analyze global data flows to generate insight and deliver effects. The IC should take immediate action to leverage these emerging capabilities to protect the nation and maintain our competitive advantage over the PRC. The IC has traditionally been at the cutting edge of adopting emerging technology but, unlike earlier technological leaps that were mostly additive in nature, GenAI will not only transform how intelligence work is done but also enable intelligence services to accomplish far more than they can today.

The IC has already taken advantage of earlier forms of AI and is using ML and NLP tools to help it manage the exponential increase in data that has overwhelmed collectors and analysts in recent years.[46] While we recognize the foundational shifts from AI as a whole, GenAI will have an even broader impact. As Large Language Models (LLMs) – multi-modal models that can generate images, video, sound, – and other forms of GenAI become more numerous, faster, more accurate, and more capable, IC agencies will come under strong pressure to adapt their approaches to every portion of the intelligence cycle, from planning and collection to analysis and dissemination.

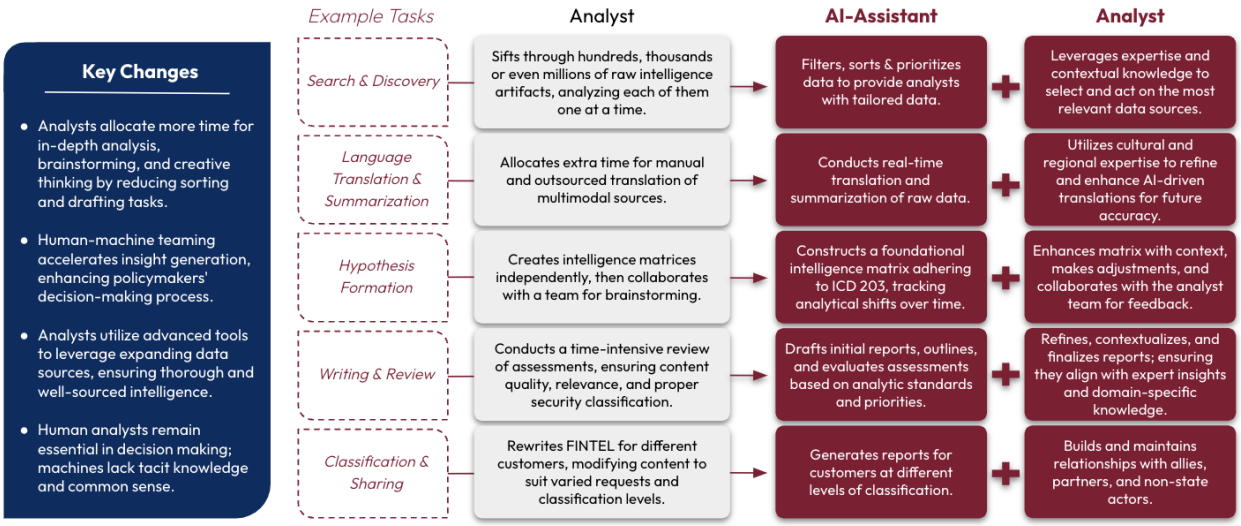
Of all the emerging technologies, GenAI stands out as an exceptionally consequential general-purpose technology warranting urgent adoption.[47] As a fundamentally "generative" technology, AI systems like ChatGPT have shown the ability to rapidly build upon their own capabilities and accelerate advances in other technology domains. The nation that acts quickly to employ GenAI for defensive and economic innovation will gain an insurmountable first-mover advantage.
For intelligence agencies, the proliferation of generative models brings both profound opportunities and risks. GenAI will provide adversaries new avenues to penetrate the United States' defenses, spread disinformation, and undermine the IC's ability to accurately perceive their intentions and capabilities. More broadly, GenAI will further democratize intelligence

[46] Since the 1980s, U.S. intelligence has recognized AI's potential for efficient data management. However, experiences with AI have been inconsistent and modest at best, delivering modest successes in speech-to-text and speaker recognition technologies. Still, the ambition to apply AI to routine tasks or vital applications across the IC has been constrained by compliance concerns and the technology's nascent stage. See more at 1983 AI Symposium Summary Report, Central Intelligence Agency(1983); Community Sponsored Plan for Artificial Intelligence, Central Intelligence Agency (1983); AI Symposium, Central Intelligence Agency(1983); Philip K. Eckman to John McMahon, Appreciation for Participation in AI Symposium, Central Intelligence Agency (1983); AI Steering Group: Meeting 4 Minutes, Central Intelligence Agency (1983); Proposal to Expand the Current APARS System, Central Intelligence Agency (1986); Philip K. Eckman to John McMahon, Intelligence Community Efforts Companion to Darpa Strategic Computing Program, Central Intelligence Agency 1984).

[47] Innovation Power for the Generative AI Flywheel, Special Competitive Studies Project (2023).

capabilities, enabling more actors to swim in the ocean of global data in pursuit of their own goals. Just as the IC currently tracks foreign leaders and institutions, intelligence services will eventually need to plan and account for AI-enabled machines acting as semi-independent actors, directing operations and making decisions, both for our adversaries and allies.

The effects of GenAI will not stop there. As AI tools become more prevalent and mature, they will put additional strain on several long-held IC practices and cultural norms, such as the relative importance of classified over unclassified data sources, legal restrictions against the use of data sources that might contain privacy and proprietary information, and what it means for something to be "secret" or "clandestine" in a global, hyper-connected, digital datasphere. Relying on unique, sensitive, and often expensive sources and methods to uncover secrets will no doubt remain a core component of what the IC does in the future. But the utility of traditional intelligence collection will increasingly be measured against what can be obtained from publicly and commercially available sources that are processed and analyzed by AI acting in partnership with humans.



Given the disruptive potential at stake, intelligence services must rapidly prototype and integrate generative AI while also evolving tradecraft to account for its complications. Inaction or delay ensures a lasting strategic setback.

Visualizing the Potential

With the appropriate governance controls in place and support from sufficient infrastructure, the rewards for moving quickly to embrace the potential of GenAI are numerous. Fully deployed LLMs would enhance the IC's performance in every stage of the intelligence cycle and enable it to cover more issues, and at greater depth.

Human-Machine Teaming: The Intelligence Cycle Reimagined

The intelligence cycle was originally designed to be continuous, with functions seamlessly passing between one another and the ability to omit steps. But it evolved into a very sequential process with extended phases, creating siloed expertise. Today, advances in GenAI could allow for a return to a more continuous, integrated cycle with fluid human-machine teaming across four key functions:

- Discover: GenAI rapidly gathers and explores massive amounts of structured and unstructured data from diverse classified and open sources.
- Generate: GenAI detects patterns, shares insights, and retains data. Humans validate sources, attribute accuracy, and assess intent.
- Fuse: Machines assemble intelligence; humans verify validity, prioritize findings, and make decisions.
- Deliver: GenAI disseminates intelligence rapidly across networks; humans control quality and appropriate use.

This human-machine teaming leverages GenAI's speed and scale with human judgment and oversight. It fills information gaps, harnesses diverse data, and provides intelligence advantages in today's dynamic environment. The cycle is no longer an isolated sequential process, but an integrated continuum enriched by human and machine collaboratively building knowledge.[48]

More fundamentally, the advent of GenAI offers the opportunity to galvanize the Community to embrace the broader cultural changes necessary to ensure its success in the digital era. Dubbed by some as the "revolution in intelligence affairs,"[49] these cultural shifts include a willingness to use AI and other autonomous systems to process huge volumes of data, reconsideration of the bureaucratic stovepipes separating the different INTs and stages of the traditional intelligence cycle, a greater openness toward the private sector (especially the sources of cutting-edge technology), and even a reconsideration of what constitutes "secret" information.

At the heart of this transformation should be open-source intelligence.[50] Unlocking the power of OSINT should up-end traditional models for intelligence collection and analysis that focused almost exclusively on the IC's unique, exquisite, and highly-classified intelligence sources and methods. Unlocking secrets will always be an important IC task, but what will matter more in a future high-speed, data-driven tech competition with the PRC will be speed-to-insight, obtained from whatever sources are available. Most of those sources will be openly or commercially

[48] VeraLinn Jamieson, Human Machine Teaming: The Intelligence Cycle Reimagined, Mitchell Institute for Aerospace Studies (2024).
[49] Anthony Vinci, The Coming Revolution in Intelligence Affairs: How Artificial Intelligence and Autonomous Systems Will Transform Espionage, Foreign Affairs (2020); The Revolution in Intelligence Affairs: Future Strategic Environment, The National Academy of Sciences (2021); Anthony Vinci & Robert Cardillo, AI, Autonomous Systems and Espionage: The Coming Revolution in Intelligence Affairs, Center for Security and Emerging Technology (2021).
[50] The Office of the Director of National Intelligence defines open source intelligence (OSINT) as "intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement." U.S. National Intelligence: An Overview 2011, Office of the Director of National Intelligence at 54 (2011).

available, and the new AI tools to exploit this data will already be trained on much of it. The IC should emphasize greater use of OSINT, making it the INT of first recourse rather than the last. Adopting and normalizing this mindset would put the IC in a better position to keep pace with what industry vendors and academic institutions will be providing U.S. policymakers, and allow it to husband its resources and fragile sensitive capabilities and target them against only the most difficult of targets.

A Critical Near-Term Challenge: GenAI-Enabled Disinformation

GenAI will amplify the threat of disinformation and foreign malign influence. As GenAI capabilities become more diffuse through open-source software, foreign adversaries will be able to leverage them to dramatically increase the quantity, quality, precision, and stealth of their influence operations.

The pro-CCP influence operation "Spamouflage" illustrates the new danger. First identified in 2019,[51] it has since leveraged AI to generate fake avatars,[52] news anchors, and fully synthetic videos promoting pro-CCP narratives – the first of their kind.[53] While not widely viewed,[54] the operation's ability to automate high-quality fake content highlights how GenAI could enable more widespread disinformation, making it harder for platforms' – let alone people – to detect.[55]

The IC will need to prioritize identifying, understanding and revealing foreign malign influence operations that will likely leverage GenAI. Timely and actionable Indications & Warnings (I&W) should inform U.S. and allied officials to counter these threats immediately after or, if possible, before they emerge.

Newly AI capabilities like classifiers[56] and similarity analysis can help the IC detect synthetic content.[57] Combining these emerging GenAI technologies with proven tactics and existing efforts, such as digital watermarking,[58] content provenance tracking,[59] and immutable ledger verification,[60] the IC can bolster efforts to identify malign influence powered by AI, assess impact, and provide actionable warnings.

[51] Ben Nimmo, et al., Cross-Platform Spam Network Targeted Hong Kong Protests: "Spamouflage Dragon" Used Hijacked and Fake Accounts to Amplify Video Content, Graphika (2019).
[52] Ben Nimmo, et al., Spamouflage Goes to America: Pro-Chinese Inauthentic Network Debuts English-Language Video, Graphika (2020).
[53] Incident 486: AI Video-Making Tool Abused to Deploy Pro-China News on Social Media, AI Incident Database (2023).
[54] Deepfake It Till You Make It: Pro-Chinese Actors Promote AI-Generated Video Footage of Fictitious People in Online Influence Operation, Graphika (2023).
[55] Ben Nimmo, et al., Second Quarter Adversarial Threat Report, Meta at 12 (2023).
[56] Steven T. Smith, et al., Automatic Detection of Influential Actors in Disinformation Networks, PNAS (2021).
[57] For example, Taiwan AI Labs uses a series of AI technologies to identify, analyze, and summarize suspected disinformation. See Infodemic: Taiwan Disinformation Understanding for Pandemic, Taiwan AI Labs (last accessed 2024).
[58] Watermarking tools may include attaching green tokens to text outputs of LLMs, hiding an image or marker inside another image, or embedding identification tones within audio. See generally, John Kirchenbauer, et al., A Watermark for Large Language Models, arXiv (2023); Eric Hal Schwartz, Resemble AI Creates Synthetic Audio Watermark to Tag Deepfake Speech, voicebot.ai (2023).
[59] Content provenance verifies the source and version history of a given piece of media. The Coalition for Content Provenance and Authenticity's (C2PA's) technical specification is a leading example from industry. See Pawel Korus & Nasir Memon, Content Authentication for Neural Imaging Pipelines: End-to-end Optimization of Photo Provenance in Complex Distribution Channels, arXiv (2019); C2PA Technical Specification, Coalition for Content Provenance and Authenticity (last accessed 2024).
[60] What is Blockchain Technology?, IBM (last accessed 2024).

Actions the IC Should be Taking Now

To fully capitalize on GenAI's potential, the IC must quickly move beyond experimentation and limited pilot programs to begin deploying GenAI tools at scale. Speed is essential. IC agencies should make it a priority to incorporate and begin using enterprise-level generative AI tools within the next two years. This is an ambitious goal, but it is achievable and essential if the IC is to stay relevant. It will require the IC – with the support of the White House and Congress – to make some critical decisions about how it will utilize GenAI, particularly whether to build its own in-house models or leverage commercially-developed models, the extent to which it builds unified or federated GenAI systems across the Community, and what standard will govern the IC's use of AI. The current U.S. administration has directed the National Security Council to prepare a new National Security Memorandum (NSM) this year to guide the IC and the Department of Defense on the safe and ethical use of AI that will begin addressing at least some of these decisions[61]. While all these issues are important to getting AI right across the IC, it will take time and further experience working with GenAI to resolve them. This should not stand in the way of the IC making progress now toward implementation.

To ensure alignment across the IC, the DNI should require that IC agencies adhere to four critical principles regarding AI implementation:

1. **Begin Using GenAI Tools Immediately.** Because GenAI will have such a profound impact on how IC professionals will go about their work, it is vital that the IC begins to make broader use of these tools immediately so that it can train its workforce and begin to create the infrastructure and policies it will need to employ LLMs safely and effectively. In part to help the Office of the Director of National Intelligence (ODNI) respond to Congressional requirements for updates, ODNI should require that IC agencies participate in a new IC-wide AI Governance Committee and demonstrate how they are contributing to or using IC-wide GenAI architectures, and/or developing their own enterprise solutions.

2. **Focus on Being an "Agile Adopter."** IC agencies are being pressed to choose between two extreme approaches when thinking about how to deploy LLMs and multi-modal models: 1) opt to do very little in-house development and instead rely on commercially-provided models for limited purposes, or 2) invest large sums of money to build state-of-the-art models at IC owned-and-operated facilities that utilize OSINT in addition to IC data holdings and seek to match the latest generations of commercial systems. There is a more balanced alternative. IC agencies should partner with foundation model providers to license their LLMs and fine-tune their training with IC-owned datasets and unique terminology, or to pair commercially-available models with smaller, IC-developed

[61] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, The White House (2023).

models. Given that many of the 'largest' LLMs do not disclose their training datasets, the IC should advance efforts by the General Services Administration (GSA)[62] to establish independent standards or rating systems for evaluating the datasets used in training (as described in the adjacent text box). This strategy would offer an effective method for assessing the resulting model's efficacy, promoting greater transparency and trust in the application of these models.

3. **Tackle Privacy Concerns Up Front.** By their nature, LLMs – particularly frontier models – include anonymized data from across the Internet, including data on U.S. persons, for training purposes. ODNI should work on getting IC agencies the necessary authorization to make use of LLMs that include personal identifiable information (PII). This may require exemptions to existing PII restrictions,[63] or it may require a creative partnership with another agency – such as the GSA – that is authorized to manage LLMs[64] on behalf of the U.S. Government. Left unresolved, IC agencies are likely to take a varied approach, with some embracing LLMs and others severely restricting their use. In addition, this will open opportunities for adversaries to "poison" LLMs with privacy or protected intellectual property data to prevent IC use.

4. **Insist on IC-Wide AI Solutions Wherever Possible.** The IC will need to strike the right balance between fostering a climate of innovation to encourage AI development across the 18 agencies and establishing coordinated approaches to achieve economies of scale. AI expertise varies across the Community and there will be a tendency for agencies to protect their unique datasets and capabilities. Left unaddressed, this could result in a proliferation of small LLMs that individually and collectively will pale in comparison to what will be used by the PRC or that will be commercially available. And the IC would achieve none of the economies of scale or uniform governance standards possible. ODNI's 2023-25 Data Strategy should serve as the model for aligning IC agencies on AI strategy.[65] ODNI should use its budget authority to insist that IC players, particularly the CIA, NSA, NGA, and DIA, cooperate to acquire near-cutting-edge LLMs from the private sector to train on their data holdings, and it should exercise its convening authority to bring the Community together to set standards for AI use. As the IC's LLM capabilities mature, there ought to be flexibility for some agencies to tailor their stand-alone, smaller models to better protect sensitive sources and methods. As long as such models are the

[62] Security Policy for Generative Artificial Intelligence (AI) Large Language Models (LLMs), General Services Administration (2023).
[63] The use of personally identifiable information (PII) by the IC must adhere to the Privacy Act of 1974 (5 U.S.C. § 552a) and additional, disparate restrictions. Governing documents also include Executive Order 12333 and Intelligence Community Directive 503 by the Office of the Director of National Intelligence.
[64] The General Services Administration issued an instructional letter (IL) to provide an interim policy for controlled access to generative AI large language models (LLMs) from the GSA network and government furnished equipment (GFE). See more at Security Policy for Generative Artificial Intelligence (AI) Large Language Models (LLMs), General Services Administration (2023).
[65] The IC Data Driven Future: Unlocking Mission Value and Insight, Office of the Director for National Intelligence (2023).

exception, not the rule, then they will add to AI's impact without inhibiting overall IC performance.

Desirable Characteristics for IC Large Language Models As IC agencies consider which LLMs to license, test, build or deploy, they should require them to fulfill at least the following criteria...	Accessible to cleared researchers, analysts, and operators for inspection and instrumentation during model fine tuning.
	Able to ingest structured and unstructured live data from various IC elements, irrespective of location (e.g., multi-cloud, hybrid, prem), modality (e.g., text, image, audio, video), or classification level (e.g., unclassified, confidential, secret, top-secret).
	Secured from revealing sensitive information, including classified data, tradecraft methods, and the content of prompts and outputs.
	Minimize the risk of being trained on sensitive data, especially proprietary or privacy information.
	Adheres to analytic and operational standards, generating accurate and relevant insights with sources that are credible and verifiable, with minimal hallucinations.

Consistent with the administration's October 2023 Executive Order, the IC's newly-appointed Chief Artificial Intelligence Officers, led by the Deputy DNI for Science and Technology, have now organized an IC Chief AI Officer Council[66] comprised of AI program managers, data owners, IT security experts, and acquisition officials from across the Community. As the IC awaits the forthcoming NSM that will provide broad guidance on its use of AI, this Council should begin exercising its convening authority to advise the DNI on AI architectures, security requirements, tradecraft standards, privacy safeguards, and intellectual property protections. To begin making decisions on LLM acquisition, governance, and use. Within six months after final publication of the NSM, the IC AI Council should complete the following:

- **Publish DNI Guidance on the Use of AI Across the IC.** The IC AI Council should produce an Intelligence Community Directive (ICD) that defines and establishes the detailed parameters that will govern the IC's use of LLMs and other AI tools.[67] Among other objectives, the new ICD should define acceptable IC uses for generative AI tools and

[66] Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, White House at 10.1(b)(iii) (2023).

[67] ODNI's Office of Augmented Intelligence Mission (AIM) would be the most logical entity to act as the executive secretariat for the Board.

provide exemptions for using private data on U.S. citizens, consistent with the guidelines established by ODNI's Chief for Civil Liberties, Privacy, and Transparency.[68]

- **Identify Steps to Remove the Obstacles to Faster Acquisition and Deployment of LLMs.** Leveraging GenAI necessitates faster technology acquisition and absorption. ODNI should exercise its full authority to shorten procurement timelines for critical emerging technologies related to LLMs. This includes finding ways to move faster in the context of the Federal government's annual budget and appropriations cycle. The IC, for example, could do so by encouraging IC element Directors, Deputy Directors, and Senior Acquisition Executives (SAE) to use Other Transaction Authority (OTA) and Commercial Solutions Opening (CSO) authorities to pursue non-standard procurement and innovative commercial capabilities or technological advances at fixed price contracts of up to $100 million, respectively.[69] To facilitate the adoption of AI technologies, ODNI should require greater transparency across elements to understand the GenAI technology acquisition environment. The status of various efforts could be consolidated into a single platform, allowing the DNI and agency leaders to identify opportunities for collaboration and places where they should amend IC acquisition authorities to increase the speed of technology adoption.

- **Establish Analytic Tradecraft Standards for the Use of Generative AI for Finished Intelligence Analysis.** The IC AI Council, in coordination with the National Intelligence Board that includes the heads of analysis from each IC agency, should articulate common standards and concepts to measure the efficacy of novel analyses produced by humans in collaboration with generative AI models.[70] The Council findings should be integrated into strategic planning and budget documents, and incorporated into existing analytic tradecraft standards, including ICD 203.[71] Meanwhile, the DNI should create incentives for analytic units across the IC to experiment with LLMs by directing relevant IC leaders to: 1) deploy OSINT-trained LLMs to analysts' computers, 2) work with the Office of Human Capital and the IC Training Council to update intelligence training to prepare all personnel for continuous machine collaboration in their careers, and 3) grant National Intelligence Program (NIP) Managers and Military Intelligence Program (MIP) Component Managers the freedom and resources necessary to accelerate HMT at the analyst level.

[68] The ethics principles and the ethics framework are meant to guide the implementation of AI solutions in the IC. See Principles of Artificial Intelligence Ethics for the Intelligence Community, Office of the Director of National Intelligence (2020); Artificial Intelligence Ethics Framework for the Intelligence Community, Office of the Director of National Intelligence (2020).

[69] Corin R. Stone, The Integration of Artificial Intelligence in the Intelligence Community: Necessary Steps to Scale Efforts and Speed Progress, Digital Commons @ American University Washington College of Law at 18-21 (2021).

[70] There was some movement in this area in the 2024 Intelligence Authorization Act where Sec. 7510 and Sec. 7513 called for a greater standardization of AI across the IC and for ODNI to brief Congress on whether current ICD standards are sufficient to address AI/ML. See Pub. L. 118-31, National Defense Authorization Act for Fiscal Year 2024 (2023).

[71] IC Directive 203: Analytic Standards, Office of the Director of National Intelligence at 1 (2015).

- **Design AI Capabilities with Allies from the Start.** The IC AI Council should plan now on how the IC will enable and empower friendly liaison services to also leverage GenAI capabilities to prevail in a long-term techno-economic contest with the PRC. Many U.S. partners such as the United Kingdom,[72] Israel,[73] the United Arab Emirates,[74] and Japan,[75] are already fostering private sector development and government use of AI-enabled tools; others are farther behind. In concert with the DNI, the Directors of CIA, NSA, and DIA should convene a consortium of AI-proficient allied states to share best practices and establish common use guidelines and principles. This consortium should broaden AI-related technical collaboration to develop shared tools. It could also be undertaken within the AUKUS Pillar II framework and ongoing AUKUS Artificial Intelligence and Autonomy working group.[76] Other possibilities include forums like the Quadrilateral Security Dialogue's Critical and Emerging Technology Working Group.[77] Because the United States is a leader in AI, such an approach would position America to help set standards for global intelligence services' use of GenAI that ensure U.S. citizens' privacy and U.S. industries' interests are better protected.

Longer-Term Efforts

These measures are the minimum necessary to start making progress toward deploying LLMs and staying ahead of the PRC, but they will not be enough to sustain the IC's leadership. Additional reforms to the IC's approach to workforce recruitment and development and how it leverages open source intelligence will be necessary to maintain the intelligence advantage in AI. Specifically, the IC should focus on:

Increasing Collection and Analysis on Foreign AI Capabilities. It is essential that the IC provide U.S. policymakers with accurate information and analysis on how foreign adversaries and competitors – particularly the PRC – are progressing in their development and deployment of GenAI tools, and how they intend to use them against us. The DNI should task collectors to devote more resources to obtaining non-public insights into foreign AI plans, and this may require a

[72] Industrial Strategy Building a Britain Fit for the Future, UK Secretary of State for Business, Energy and Industrial Strategy (2017); Regulatory Sandbox Final Report: Onfido Limited (Onfido), Information Commissioner's Office (2020).
[73] Yaniv Kubovich, Israeli Air Force Gets New Spy Plane, Considered the Most Advanced of Its Kind, Haaretz (2021); Anna Ahronheim, Israel's Operation Against Hamas was the World's First AI War, The Jerusalem Post Customer Service Center (2021).
[74] UAE National Strategy for Artificial Intelligence 2031, Government of the United Arab Emirates (2017); UAE Council for Artificial Intelligence and Blockchain, Government of the United Arab Emirates (2021); The Artificial Intelligence Program, Government of the United Arab Emirates (2020).
[75] New Robot Strategy, Japanese Ministry of Economy, Trade and Industry, Headquarters for Japan's Economic Revitalization (2015); Impacts and Risks of AI Networking—Issues for the Realization of Wisdom Network Society, (WINS), Japanese Ministry of Internal Affairs and Communications, Telecommunications Research Laboratory (2016); Fumio Shimpo, Japan's Role in Establishing Standards for Artificial Intelligence Development, Carnegie Endowment for International Peace (2017).
[76] FACT SHEET: Implementation of the Australia – United Kingdom – United States Partnership (AUKUS), The White House (2022).
[77] Quad Critical and Emerging Technology Working Group, Australia's Department of Foreign Affairs and Trade (2021); Husanjot Chahal, et al., Quad AI: Assessing AI-related Collaboration between the United States, Australia, India, and Japan, Center for Security and Emerging Technology (2022).

tighter lash-up between HUMINT and technical collection experts and the IC's analytic experts on AI to better refine the IC's targeting. The DNI also should task the National Intelligence Council (NIC) to assemble a network of IC all-source analytic experts to assess foreign development and use of LLMs and other GenAI tools. The NIC should organize a cross-IC Red Team to also consider how the PRC or other adversaries would seek to forestall, or undermine, the U.S. Government's use of LLMs and to augment their ability to conduct cyberattacks against our infrastructure and ramp up their disinformation operations targeting U.S. citizens.

Building an AI-Ready IC Workforce. The key to harnessing GenAI's potential for securing an intelligence edge resides in the IC's people – from the developer to the end-user. The IC cannot afford to "buy" external expertise. To stay abreast of the fast-paced advancements in GenAI and related technologies, the IC must attract the right talent while also sharpening the digital acumen of its existing cadre of intelligence professionals. The DNI should delegate the ADNI/IC Human Capital to undertake four key measures:

1. **Establish a universal "AI technical competence" standard for intelligence elements.** These should incorporate new and existing AI skills defined by the Office of Personnel Management (OPM).[78] The DNI should also update and harmonize directives[79] with workforce strategies and existing technology-centric talent exchange programs such as the IC's Intelligence Learning Network,[80] Civilian Joint Duty Program,[81] and the Public-Private Talent Exchange.[82]

2. **Build official career tracks for AI tech talent across the IC.** In coordination with the OPM and the Office of Science and Technology Policy (OSTP), the IC should develop one or more occupational series, associated policies, and official position titles related to GenAI and digital career fields Descriptive parenthetical titles should be introduced to accurately identify IC software professionals in the short-term This immediate step will assist IC talent management strategies for attracting and retaining GenAI tech talent.

3. **Revamp analytic incentives.** The rise of GenAI will transform how analysts go about their work. New tools will enable analysts to contend with the mountains of

[78] Kiran A. Ahuja, Memorandum For Chief Human Capital Officers, Office of Personnel Management (2023).
[79] ICD 651, Performance Management for the Intelligence Community Civilian Workforce, Office of the Director for National Intelligence (2017); ICD 656, Performance Management System Requirements for Intelligence Community Senior Civilian Officers, Office of the Director for National Intelligence (2012).
[80] Pub. L. No: 108-458, Intelligence Reform and Terrorism Prevention Act of 2004 § 1041(c).
[81] ICD 660, IC Civilian Joint Duty Program, Office of the Director for National Intelligence (2013); ICD 651, Performance Management System Requirements for the IC Civilian Workforce, Office of the Director for National Intelligence (2012); IC Standard (ICS) 660-02, Standard Civilian Joint Duty Application Procedures, Office of the Director for National Intelligence (2018).
[82] ICPM 2022-600-02, Intelligence Community Public-Private Talent Exchange, Office of the Director for National Intelligence (2022).

data available, but human experts will need to adjust their approach and learn to partner with machines to be successful. Rather than spending their time painstakingly searching through reports to find relevant data, analysts increasingly should oversee AI Agents – autonomous software skilled at web navigation, information validation and disinformation detection, and keeping track of ever-evolving customer requirements – to discover new information and discern when the data support alerting customers to potentially valuable new insights.[83] This will require a different, more proactive mindset to manage these networks of virtual AI Agents on the one hand, and an increased willingness to trust that what these Agents are saying is new, important, or otherwise relevant to policy consumers.[84] To ease this shift, the IC must revamp its training initiatives, equipping analysts with the essential skills and tools to handle GenAI-centric tasks, including guiding AI Agents towards making better discoveries.

4. **Leverage American expertise in GenAI as a national resource for IC competitive advantage.** The IC should encourage technical experts leaving the IC to join the National Intelligence Reserve Corp (NIRC),[85] while simultaneously establishing new volunteer avenues for private sector technology specialists to become part of the NIRC, effectively serving as a "digital reserve force."[86]

Reinvigorating the Open Source Mission. To get the best use out of LLMs, particularly foundation models that are trained on vast amounts of OSINT data, the IC needs to dramatically increase its access and use of OSINT of all kinds, including commercially available information. As a first step, ODNI should empower the new position of OSINT Executive to harmonize the use of OSINT across the enterprise and to identify successful programs and advocate for them to receive greater resources. But this step alone is unlikely to overcome IC agencies' reluctance to make OSINT a priority or deliver the variety or quality of OSINT information required. ODNI should also begin pursuing alternative solutions, including the possible creation of a new Open Source Agency (either within the IC or outside of it), with a new public-private partnership with industry to gain greater access to the private sector's growing capabilities as an interim step.

[83] For more on AI Agents and similar systems, see Kyle A. Kilian, et al., Examining the Differential Risk from High-Level Artificial Intelligence and the Question of Control, Futures (2023).

[84] A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis, National Academies of Sciences, Engineering, and Medicine at 6, 189–238, 312–315 (2019); Nick Hare & Peter Coghill, The Future of the Intelligence Analysis Task, Intelligence and National Security at 858–870 (2016); Efren R. Torres-Baches & Daniela Baches-Torres, Through the Cloak and Dagger Crystal Ball: Emerging Changes that will Drive Intelligence Analysis in the Next Decade, Journal of Mediterranean and Balkan Intelligence at 161-186 (2017).

[85] Established under the Intelligence Reform and Terrorism Prevention Act of 2004. ICPM 2006-600-1 - National Intelligence Reserve Corps, Office of the Director for National Intelligence (2006).

[86] Final Report, National Security Commission on Artificial Intelligence at 10 (2021).

A New Tech-Enabled Vision for IC Partnerships

Since World War II, the U.S. Intelligence Community has created a global network of foreign intelligence liaison relationships with democratic allies and other friendly states to share intelligence and, in some cases, to conduct joint intelligence operations or to co-develop new collection capabilities. The higher-profile set of relationships are the multilateral sharing agreements with our key allies such as the "Five Eyes" arrangement that includes the United States, UK, Australia, Canada, and New Zealand. This also includes intelligence sharing within the NATO alliance and the recently-created Australia-United Kingdom-United States (AUKUS) Partnership.[87] In addition to these multistate structures, the IC has knit together an intricate web of bilateral arrangements that are carefully tailored to fit the parameters of Washington's diplomatic ties to various key states. Some relationships, such as with Japan, the Republic of Korea, Israel, and Colombia, are robust while others may be weaker.

Recognized by the White House as "our most important strategic asset" for U.S. national power, these security relationships have enabled the IC to extend its reach, gain an information advantage over adversaries, detect and thwart threats, and to support policy-led efforts to create a shared sense of purpose with friendly and allied states.[88] The IC, at the direction of successive U.S. Presidents, has also formed discrete intelligence liaison exchanges with neutral states and geopolitical competitors, including the PRC and Russia, to allow for quiet exchanges on mutual threats such as illegal narcotics trafficking or terrorism. These linkages have proven valuable even during periods when official bilateral relations were frosty, both as a foundation upon which to eventually rebuild communication and cooperation and as a trusted conduit to directly communicate intentions during a crisis.

Over the years, the IC has developed a similarly robust set of partnerships with a wide variety of organizations here in the United States. The domestic landscape is in some ways even more complex than the foreign environment, with U.S. intelligence agencies interacting with private sector companies and businesspeople, academic institutions, state and local governments, and private citizens. In some cases, these relationships are transactional in nature, while other ties may be more collaborative and enduring (such as joint research with U.S. National Labs). The rules and restrictions placed upon the IC as it conducts these outreach efforts can often be

[87] A Brief History of the UKUSA Agreement, Government Communications Headquarters (2021); Michael S. Goodman, The Foundations of Anglo-American Intelligence Sharing: Evolution of a Relationship, Studies in Intelligence at 1-12 (2015); Michael E. DeVine, United States Foreign Intelligence Relationships: Background, Policy and Legal Authorities, Risks, Benefits, Congressional Research Service (2019); Gabriel Dominguez, Philippines Considering Trilateral Defense Pact with U.S. and Japan, Japan Times (2023).

[88] National Security Strategy of the United States, The White House at 11 (2022).

onerous, reflecting the sensitive nature of the work or the potential risk to U.S. companies or individuals that can result from their support to the IC.

While the IC's network of foreign and domestic partnerships proved extremely effective at blunting Soviet military power during the Cold War and at driving the United States' post-2001 campaign against global terror threats, the Intelligence Community needs to take a fresh look at how its partnerships are structured and managed to support Washington's next great challenge: prevailing in the techno-economic competition with PRC. Unlike the Cold War or the Global War on Terror, this competition will be less about gaining tactical military advantages to deter aggression or to eliminate threats and will be more broad-based involving all elements of U.S. society to protect the health and vibrancy of our private sector and of our democratic institutions. This decade likely will decide which societies have dominance in the key technological frontiers that will shape the global economy and balance-of-power for the next generation.[89] Whoever comes to dominate these technologies – including GenAI, next generation microprocessors and communications networks, advanced manufacturing, energy storage and production, and biotechnology – will gain enormous economic advantages, increase their relative national power, and potentially set the rules by which others gain access to these tools. In this environment, the intelligence insights that will matter in the future will likely come less often from uncovering the hidden plans and intentions of foreign governments and bad actors (though those will still matter greatly) and instead will come more frequently from the corporate boardrooms and private labs that are creating the wave of transformative technologies to come.

Laid against this new benchmark for national competition, the IC's current approach to partnerships is increasingly ill-suited to the task. The current model assumes a technology and resource environment in which the U.S. Intelligence Community is the dominant global player and the key source of innovation, and that the primary purpose of foreign liaison work was to expand the reach of IC collection and zealously protect the IC's unique sources and methods. But the IC no longer sits alone atop the technology pyramid. The increasingly widespread availability of data and the proliferation of digital and hardware tools to exploit them is democratizing intelligence and accelerating the shift of innovation away from governments and towards private industry. This disruption of the technology hierarchy means that in some instances a foreign liaison partner – not the IC – is the source of technical advantage, data, or insight.

[89] Remarks by National Security Advisor Jake Sullivan on the Biden-Harris Administration's National Security Strategy, The White House (2022).

The New Ecology of 21st Century Intelligence Relationships

- Foreign liaison partners are now less dependent on the IC to fill their intelligence collection gaps and many are growing more capable of contributing information and analytic insight, but U.S. decision makers are unable to leverage them because they are either fed into the IC's antiquated collection processes which treat most liaison reporting as suspect or they are ignored altogether.[90]

- The IC's deep network of global foreign liaison ties positions it to bolster allies' resistance to malign PRC influence and to stay ahead of the curve on technology innovation, but the IC's presumption that it still dominates the information realm and its emphasis on counterintelligence (CI) and shielding sources and methods preclude it from taking full advantage of this resource. The IC needs to place more emphasis on building and leveraging foreign partnerships to forge an international tech-based coalition of intelligence services from across the free world to drive strategic insight, prevent disinformation, and develop new tools to counter the PRC.

[90] While technical agencies, such as NSA and NGA, have made strides in updating their networks to accommodate sharing of large amounts of data with foreign partners in the past decade, this is still not being done at the scale current demands require.

Similarly, the IC's traditional methods for interacting with domestic actors, private companies, and partners are now somewhat insufficient in providing the IC with useful insights into the new ideas, technologies, and capabilities emerging from the private sector or from local governments or nongovernmental institutions that are playing an increasingly important role in setting standards and defending against threats. Most critical for the United States' ability to stay competitive over the long term, the IC remains relatively slower in incorporating and utilizing new technologies, particularly as compared to the PRC. Beijing's ability to strong-arm private industry and academia into supporting its intelligence services is nothing the United States should emulate, but the IC must find new ways to partner with our domestic innovators to stay in the game.

- A first step would be to revamp the IC's acquisition and procurement rules and practices for data acquisition and software tools to allow for much more rapid intake and deployment of new data sets and tools with speed being the critical measure of success.

- Adjusting the current process will not be enough; rather, the IC must also fundamentally rethink its approach for incorporating cutting edge technologies, like generative AI, and open source and commercially available data sets that are already being deployed across the private sector and by foreign powers.

Elevate The Foreign Intelligence Liaison Mission

U.S. foreign intelligence liaison ties are a key component of U.S. international relations. No single nation can face these threats alone. Now more than ever, the IC must leverage its expansive network of international allies and partners. Only by marshaling our collective strengths can we build a just, sustainable world order. Through efforts like the exchange of information, basing rights, burden sharing, joint operations, and training, U.S. and foreign intelligence services have been able to leverage each other's strengths to provide tactical, operational, and strategic intelligence that they would otherwise not be able to obtain alone.[91]

Traditionally, U.S. intelligence relationships with foreign counterparts have been organized in a hub-and-spoke model, with the United States at the center with separate, bilateral foreign intelligence ties radiating out from it. This maintained Washington's freedom of maneuver as individual relationships waxed and waned, and made it easier to ensure security. The two key exceptions to this approach were the IC's participation in multilateral exchanges with the so-called "Five Eyes" (United States, UK, Australia, Canada, and New Zealand) and within the NATO alliance. U.S. participation in newer multilateral arrangements has come more gradually. For example, when organizing the U.S.-Japan-ROK partnership, a Trilateral Information Sharing Arrangement (TISA) to boost coordination in dealing with regional threats, the United States intentionally restricted membership and made itself the central coordinating player to safeguard

[91] See e.g., British-U.S. Communication Intelligence Agreement, National Security Agency (1946).

its own freedom of action.[92] Other U.S. networks limited by their hub-and-spoke shape include U.S. agreements in the Indo-Pacific, like the Quad and recently formed AUKUS, which are strengthened by hundreds of other bilateral intelligence ties with countries in the region.[93]

Guidelines for managing these relationships and defining roles are found in statute, executive orders, and intelligence directives. Formal agreements, for instance, underpin most partnerships, with the IC utilizing multiple classified, non-binding memorandums of understanding (MOUs) for intelligence exchange, whereas the Department of Defense employs General Security of Military Information Agreements (GSOMIAs) and memoranda of understandings for sharing military information. U.S. government officials can disclose[94] or "release"[95] intelligence to foreign entities only if doing so is in the national interest, supports U.S. treaties and agreements overseas, the recipient can adequately protect the information, and the anticipated benefits outweigh the potential damage of a likely compromise.[96] These MOUs and GSOMIAs often serve as the foundation for wider security agreements. While the Director of National Intelligence oversees policy and approvals, IC elements can make their own partnership agreements. The CIA is the center of gravity for managing foreign intelligence liaison relationships, both by Executive Order 12333[97] and by virtue of its worldwide presence and established network of relationships and overseas infrastructure.

Limitations

Today's frameworks for foreign intelligence relationships are largely built upon historical ties with major powers, often overlooking the potential of forming new alliances with smaller nations that may possess a comparative advantage in specific capabilities. However, advancements in and the diffusion of emerging technologies are both changing the nature of the threat and democratizing intelligence capabilities.[98] During the Cold War, states leveraged their financial and industrial power to create an intelligence advantage between themselves and other actors,

[92] Joint Statement of the 13th Defense Trilateral Talks, U.S. Department of Defense (2023); Wendy Sherman, Joint Statement on the US-Japan-Republic of Korea Trilateral Ministerial Meeting, U.S. Department of State (2023).
[93] Joint Statement of the 2023 US–Japan Security Consultative Committee ("2+2"), U.S. Department of Defense (2023); Leaders' Joint Statement in Commemoration of the 70th Anniversary of the Alliance between the United States of America and the Republic of Korea, The White House (2023).
[94] ICD-403 defines "disclosure" as "displaying or revealing classified intelligence whether orally, in writing, or in any other medium to an authorized foreign recipient without providing the foreign recipients a copy of such information for retention." See more at ICD-403, Foreign Disclosure and Release of Classified National Intelligence, Office of the Director of National Intelligence (2013).
[95] In accordance with ICD-403, "release" is "the provision of classified intelligence, in writing or in any other medium, to authorized foreign recipients for retention." See more at ICD-403, Foreign Disclosure and Release of Classified National Intelligence, Office of the Director of National Intelligence (2013).
[96] The DNI is the final arbiter in resolving any disputes on what can be disclosed or released. See more at ICD-403, Foreign Disclosure and Release of Classified National Intelligence, Office of the Director of National Intelligence (2013); ICPD-403.1, Criteria for Foreign Disclosure and Release of Classified National Intelligence, Office of the Director of National Intelligence (2013).
[97] Central Intelligence Agency Authorities: Procedures Approved by the Attorney General Pursuant to Executive Order 12333 , Central Intelligence Agency at 2.2.1 (e) (2017).
[98] David V. Gioe & Ken Stolworthy, Democratised and Declassified: The Era of Social Media War is Here, Engelsberg Ideas (2022); Author Amy Zegart on the Future of American Intelligence, Intelligence Matters (2022).

both state and non-state.[99] The falling costs of computing and the rise of software-driven innovation have led to a vibrant marketplace featuring new products and services with advanced intelligence capabilities like social media and telemetry analytics, real-time earth observation, large-scale information storage and processing, mobile phone location data, and global HUMINT platforms. Such a marketplace has been cultivated largely outside of government by corporations, individuals, and even civil society organizations. Today, any actor with the sufficient will, resources, and expertise can harness these capabilities to rival well-funded intelligence agencies.

The democratization of intelligence tools and capabilities, however, has enabled a greater range of individuals to collect information and deliver intelligence products in an impactful way, fundamentally restructuring the intelligence landscape and eroding states' ability to achieve information and decision supremacy on their own. This monumental shift necessitates a reassessment of the prevailing frameworks that guide foreign intelligence relationships and a reimagining of the landscape for intelligence gathering and analysis.

- For the U.S. Intelligence Community, this means shifting from its hub-and-spoke models for doing business to a distributed intelligence network architecture in strategic theaters and sectors across the globe. With their greater number of ties between members, distributed intelligence networks are more resilient in the face of a range of different threats, and better at amplifying U.S. influence with fewer costs.[100]
- Stronger relations with states that are currently unaligned or hedging, in the Near East, Africa, and South East and Central Asia for instance, could provide significant advantages for U.S. economic and security interests in the form of access to natural resources, markets, strategic locations, or inputs to innovation. The most effective networks will form where these countries and their businesses, scientists, and other stakeholders are already interacting and around their shared needs, not necessarily around U.S. priorities.

While the United States will always have incentive to utilize foreign intelligence relationships to protect its national security by filling critical information gaps and enabling covert action, the priority in the future should be on leveraging these ties to support United States-led efforts to constrain Chinese economic and technological dominance and to fortify global partners against encroachments from Russia, Iran, North Korea, and other autocracies. In this arena of global economic and technological competition, rapidly exchanging assessments and generating collective insight into adversaries' mercantilist policies, capabilities, and intentions derived from publicly available sources – and quickly countering disinformation about the United States and its

[99] Warren Chin, Technology, War and the State: Past, Present and Future, International Affairs (2019).
[100] Anne-Marie Slaughter, The Chessboard and the Web: Strategies of Connection in a Networked World, Yale University Press (2017).

allies – will count at least as much as intelligence collection. But as currently organized, U.S. intelligence relationships are poorly-suited to support this strategic messaging mission.

- By design, the IC's hub-and-spoke model promotes transactional relationships in which the value of a particular partnership is judged solely on the exclusivity and utility of the intelligence received. With few exceptions, the relationships are not guided by how well they shape other countries' views and policies toward China and Russia.

- Because "secrecy" is the coin of these relationships, all parties have incentive to gain as much access as possible to partners' information while minimizing how much is shared in return. The impact and value to overall U.S. interests of what is shared with partners is given little consideration, and the process for expanding what is released to foreign partners is purposefully designed to be arduous.

- While the White House and policymakers in recent years have taken more of a guiding hand in determining what U.S. intelligence should be declassified or released to foreign partners (most notably as part of Washington's campaign to bolster Ukraine), the day-to-day responsibility for managing foreign intelligence relationships is delegated to the IC, which is not responsible for U.S. strategic messaging.

Recommendations

Forge a broad network of intelligence partnerships across the free world to counter authoritarian regimes. To better cope with the anti-democratic, anti-competitive influence being exerted by Beijing, Moscow, and other authoritarian regimes, the IC should lead the way in re-energizing and expanding information sharing and operational collaboration amongst the intelligence services of free societies. These partnerships should be broad-based and mutually beneficial, and with a strong focus on leveraging open source data and technologies.

> **Create a new Deputy Director of National Intelligence for Techno-Economic and Strategic Competition to lead this effort.** This would underscore the importance of national competitiveness to the IC's overall mission and provide a new lens through which to focus intelligence cooperation with friendly foreign liaison services. To be effective, the position should be imbued with real authority to help organize and prioritize the IC's foreign liaison engagements. This should include making decisions about what information and data to share with foreign intelligence services on anti-competitive trade and investment practices by authoritarian states, supply chain threats, attempts by adversaries to avoid international economic sanctions, cyber and disinformation attacks, and other transnational trends. This official would serve as the IC's touchpoint to work with the policy community to coordinate and direct declassification of U.S. intelligence and private sharing of U.S. intelligence with trusted partners to achieve strategic impact.

Conduct a strategic review of opportunities for new regional intelligence sharing frameworks that would advance U.S. and allied interests. The Deputy Director of National Intelligence for Techno-Economic and Strategic Competition, should undertake a strategic review of opportunities for new regional intelligence sharing frameworks that would advance U.S. and allied interests. Based on this review, the DNI should direct relevant IC agencies to engage with partner nations to establish formal arrangements modeled on successful frameworks like the Five Eyes and AUKUS. Initial focus areas should include:

- Middle East – Build on the Abraham Accords to increase collaboration between Israel and Arab partners. Seek funding for joint analytical cells and secure communications.
- Asia – Enhance intelligence ties with and capacities of Japan, South Korea, India, The Philippines, and Vietnam to counter China. Setup reciprocal exchanges of assessments on Chinese military, economy, and foreign influence.
- Africa – Strengthen partnerships across the Sahel, East Africa, and Southern Africa to counter terrorism and improve stability. Provide capacity building support as needed.
- Americas – Expand long standing relationships with Canada, UK, Australia, and New Zealand. Forge new ties in Latin America around issues like migration, organized crime, and election interference.

Incentivize and hold partners accountable for the quality and relevance of their contributions. The DNI, in partnership with the proposed Deputy Director of National Intelligence for Techno-Economic and Strategic Competition, should implement a regular review process to assess the quality and relevance of the intelligence it receives from foreign partners. For partners not meeting standards, such as providing high-quality intelligence, the IC should provide technical assistance and training to improve its capabilities. The IC should also be prepared to terminate relationships with uncooperative partners to incentivize contributions.

Lead in helping friends and allies improve their security practices. The IC should work with its foreign partners to improve their security practices. This includes sharing best practices, providing training on how to protect sensitive information, and developing international encryption standards to ensure the IC can continue to access encrypted communications, while also protecting the privacy of individuals. And the IC should also be prepared to provide assistance to partners who are experiencing security breaches. Strong security practices among allies will better safeguard shared intelligence.

Facilitate reciprocal access to data for IC experts, partners, and customers. The IC should make it easier for its experts, partners, and customers to access data. A key priority of any approach should be expanding the use of open source intelligence by investing in tools and training, establishing incentives, sharing OSINT reports with domestic partners, and collaborating responsibly with tech companies. However, while the lawful and ethical expansion of OSINT is a fundamental part of this effort, it is not the only action needed.

Normalize "write for release" as the default for IC analytical products and assessments. Dissemination of finished intelligence assessments on techno-economic topics and certain transnational issues, such as climate change or refugee flows, should no longer default to "Not Releasable to Foreign Nationals (NOFORN)" or "Releasable only to the Five Eyes: USA, Australia, Canada, New Zealand, and the United Kingdom (FVEYs)." Instead, the DNI should make broader dissemination the new norm for these analytical products to facilitate increased sharing of intelligence with allies and policymakers without needing lengthy review and clearance processes. To implement this, IC elements should:

- Set goals for increasing the percentage of assessments reproducible for release. Establish new abbreviated review processes for release-ready products. Update report templates and style guides to conform to "write for release" from project inception.
- Train analysts on writing for public release and protecting only limited classified sources, and incentivize authors and managers to maximize release-ready content.
- Automate sanitization where feasible using natural language processing.[101]

Create and foster technology-enabled collaborative spaces with FVEY partners and a select few close U.S. allies to pool intelligence, conduct joint assessments, and tackle shared challenges. The DNI should establish secure virtual technology-enabled collaborative platforms and spaces to enable the Five Eyes and select allies to collaboratively pool intelligence, conduct joint assessments, and tackle shared challenges. IC tech teams should develop access controls to compartmentalize information among partners. The U.S. Government should ensure appropriate funding for these digital collaboration spaces.

Build more infrastructure for bilateral and multilateral secure communications. The IC Chief Information Officer should expand infrastructure for secure multimedia communications to allow bilateral and multilateral engagements between intelligence agencies. This should include scaling up secure video teleconference capabilities and deploying user-friendly interfaces.

[101] AI's Role in Reimagining the Classification System, Medium (2024).

Create "data lakes" in a cloud environment to share large datasets and collaborate on joint analyses that can be made available to all partners. The DNI, in partnership with the proposed Deputy Director of National Intelligence for Foreign Partnerships, should establish a program to develop federated "data lakes" in a secure cloud environment to enable controlled data sharing with allies. These data lakes should pull structured and unstructured data from across IC agencies and databases using curation tools and AI. Robust access controls must allow configurable sharing with select partners. Key focus areas should include:

- Terrorism: Share travel, communications, and watchlist data to improve tracking of suspects globally.
- PRC: Pool economic, scientific, and defense intelligence to better understand challenges posed.
- Cybersecurity: Combine threat indicators, attack data, and best practices to enhance collaboration.
- Climate: Collect environmental data to jointly assess impacts on security.

In addition, partner nations should be encouraged to contribute data to reciprocally benefit all participants. Common analytics environments should allow collaborative projects and AI-assisted analysis.

Change The Paradigm for Domestic Partnerships

Today, the United States' competitive edge increasingly depends on the IC's aptitude at both protecting classified national security information and tapping into the innovation and creativity happening outside of the IC in order to ensure its relevance in the years ahead. The Intelligence Community needs to partner better with a broad spectrum of stakeholders across the federal government, state and local authorities, law enforcement, and with those elements of the private sector, academia, and civil society that are leading the way on innovation.

For its part, the Intelligence Community has evolved its network of relationships to meet changing geopolitical realities and evolving definitions of national security. Once focused almost exclusively on federal agencies, the IC now interacts with a diverse range of domestic stakeholders, including non-national security government agencies, private industries, academic institutions, national laboratories, and individual U.S. citizens.

The IC’s mission is to ensure the U.S.’s national security by providing timely and crucial information to its “customers” such as civilian U.S. government agencies, state and local authorities, and when necessary, the private sector. In support of these customer-based relationships, the IC disseminates relevant information, such as reports on threats, assessed vulnerabilities, and the capabilities of foreign malign actors to inform customer decisions. Public-

sector customers – which are the IC's primary customers– provide unique perspectives, directives, and potential sources that enable the IC to fulfill national intelligence requirements. IC communications to the private-sector are often akin to public service announcements, carefully tailored so as not to confer advantage to any particular U.S. individual, company, or locale (though exceptions are made when conveying threat information against U.S. persons who are being targeted). Customer-based relationships are essential for developing a common understanding of the threat environment below the federal level and for harmonizing efforts to keep U.S. citizens safe, its economy and critical infrastructure secure, and its democracy resilient. However, customer-focused relationships, though seemingly vast in their scale, do not always translate to widespread action.

Commercial-based relationships are a key tool for the IC to acquire specialized data, insights, and cultural, military, or linguistic contracting services that are otherwise unattainable or prohibitively expensive to develop in-house. These relationships are primarily transactional and driven by the IC's immediate intelligence or resource needs. These interactions typically transpire through controlled channels due to the proprietary nature of the procured products and services. Commercial-based relationships are essential for quickly gaining access to new technologies and expertise. However, this might come at the expense of developing in-house capabilities.

Partner-based relationships are characterized by a high degree of collaboration and cooperation over a sustained period of time. While there is no legal definition of what constitutes a domestic partner of the IC, these relationships, either for profit or voluntary, strive towards shared objectives. The reciprocal nature of these interactions fosters a mutually beneficial environment, where both the IC and its partners draw significant advantages from the cooperative arrangement to achieve common goals. Partner-based relationships cultivate enduring collaborations, igniting the potential for novel intelligence competencies. At the same time, relationships centered on partners necessitate sustained dedication, trust, and joint growth, potentially requiring a significant investment of resources and time that may not always be on hand.

	Customer-based	Commercial-based	Partner-based
Collaboration	Low	Low	High
Risk	Low	Medium	High
Cost	Low	Variable	High
Timeframe	As Needed	Short Term	Long Term
Strengths	Broad Reach, Low Cost	Quick Access to New Technologies and Expertise	Mutually-Beneficial, Potential for Novel Intelligence Innovation
Weaknesses	Lack of Personalization, Limited Depth of Information	Over-reliance on External Partners, Loss of In-house Capabilities, CI Risks	Sustained Dedication, Trust, and Joint Growth

Limitations

The Intelligence Community's current model of domestic partnership interactions is fraught with several limitations that confer advantage to Washington's more agile global competitors. First, the necessity of protecting classified information and systems can impede fruitful data exchange with domestic partners, even when it's pivotal in threat response or prevention. Second, legal constraints can restrict what the IC shares, especially if it risks violating privacy or jeopardizing national security. Third, resource constraints mean that the IC must prioritize its partnerships, potentially overlooking some domestic entities that could provide valuable intelligence or expertise. Fourth, the IC's obligation to protect sensitive sources and methods can be a barrier to fostering trust with domestic partners, thereby limiting access to crucial information and cooperation.

There have been numerous studies and previous well-intentioned efforts by the IC, successive administrations, and Congress to address these shortcomings. Few have succeeded in making more than a marginal difference to how the IC goes about working with domestic partners (with the post-9/11 reforms on domestic information sharing on counterterrorism and more recent IC-led changes to engaging private industry on cyberthreats being notable exceptions). This is likely because the various prescriptions did not fully take into account the profound impact that technological change is having on the information environment, which has in turn radically shifted the value proposition for traditional intelligence collection and analysis. Whereas before the IC could safely rely upon its near-monopoly over the means for exerting information dominance and delivering insight to policymakers, this is no longer the case today. Commercial firms, non-government organizations, universities, national labs, and a rapidly expanding list of foreign countries are challenging – and in some cases, surpassing – the IC's ability to deliver value-added insights. And they are doing so at a pace the IC finds difficult to match. A wave of publicly and commercially available information accessible on the Internet has radically altered the data landscape. On the one hand, it is now possible to collect and accurately assess many of the key international developments and trends without needing to rely on expensive, bespoke collection systems. But in order to be competitive, the IC needs to collect and analyze open source data much more quickly, and to do that it needs to harness the entrepreneurial, market-driven capabilities of the private sector. In the information domain of the future, speed-to-insight will be the coin of the realm; much more so than having incrementally more precise information.

Recommendations

Create the infrastructure and authorities to facilitate a broader exchange of information. The IC can create the infrastructure and policies necessary to facilitate a broader exchange of information between IC agencies and state and local authorities, federal civilian regulatory agencies, academia, and the private sector. This will help to enhance national competitiveness with and resilience against enduring and emerging threats.

Establish a new National Intelligence Capital Office. A new National Intelligence Capital Office (NICO) should be established under the DNI with its head reporting directly to the Principal Deputy Director for National Intelligence. The NICO would be funded by the IC, which would also appoint its director and members of the board, and set its strategic priorities. Similar to the Office of Strategic Capital at DoD, or the Foundation for the National Institutes of Health, the NICO would also be authorized to attract funding from the private sector for scaling technological solutions that are being developed in the private sector, but that have demonstrated applicability for the intelligence community. The NICO would not focus on discovering and incubating promising new technologies, a role currently being filled by IQT. Rather, it would prioritize the scaling and fast tracking of tech solutions. It would work with industry, particularly smaller companies, to help it address U.S. Government needs as it brings new solutions to market.

Create a new Digital Experimentation and Transformation Unit within the Office of the Director for National Intelligence. This entity would run pilot projects that address Community-wide challenges on talent, processes, technologies, or acquisition as identified by the DNI or IC agency directors. The purpose would be to identify and apply the best available technology and expertise – from either inside or outside of government – to select Community-wide problems.

Formulate policies that expedite the integration of AI across all levels of the IC. Although the IC stands to gain the most from AI across the government, it still appears to be moving slowly in adopting these innovations. Policies that prioritize analytic outreach are urgently required to accelerate the use of AI and to fully tap into its benefits and efficiencies.

Create more incentives and programs for IC experts to do short enrichment rotations outside of the IC to deepen their knowledge and skills. These "externships" should be done across a broad spectrum of private sector companies, non-government organizations, and academic institutions. IC experts should be incentivized to augment their tradecraft skills with experiences in the private sector as they progress through their career.

Expand opportunities for private sector experts to serve in the IC. While the IC cannot compete with the private sector on a salary basis, it offers the best avenue for technologists and subject matter experts to shape the U.S. Government's perceptions of foreign and security challenges. The IC should put itself in a position to tap the desire that many technical experts have to engage in public service by offering internships and other short-term contracts. Private sector candidates should be vetted and cleared, but once they are they should be given regular access to IC tools and data and encouraged to recommend new solutions.

Accelerating the IC's Use of Open Source

For U.S. national security to thrive in this new era, the IC will need better access to and understanding of data and insights from open-source systems outside of the U.S. Government purview at the speed and scope of mission demands. The United States' prime nation-state adversaries – China, Russia, and others – recognize the value to be found in open-source systems, and China both simultaneously harvests available U.S. data and works to protect its systems through draconian measures to wall them off from the world. A June 2023 report by Recorded Futures notes that "The People's Liberation Army (PLA) is using new collection, processing, and analysis technologies to exploit the massive amount of open source data available from the Internet and other sources for military intelligence purposes. A growing ecosystem of private companies, state-owned research organizations, and universities is supporting the PLA's push to leverage open source intelligence by providing research services, platforms, and data."[102]

China and Russia also successfully operationalize open source data against U.S. interests while using digital interconnectivity to weaken the underpinnings of our democracy and erode faith in U.S. institutions. The Senate Select Intelligence Committee has completed extensive investigations with over 1,000 pages of information on Russian interference in U.S. elections.[103] As part of these investigations, then-Senator Richard Burr (R-NC) noted that two Russian Facebook pages organized both a protest and counter-protest in front of an Islamic center in Houston in 2016.[104] Finding a way to counter them at speed and scale is vital. Beyond nation-state adversaries, non-government entities and individual open source investigators already are rapidly and conclusively revealing insights previously only the domain of nation states, including exposing U.S. and other government secrets.

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. Sophisticated adversaries and technically literate individuals will continue to pursue and act on these insights whether or not the United States does. For us to combat them, the U.S. national security community has to become as adept at understanding the open world as it is the world of classified intelligence.

Since the creation of the CIA under the National Security Act of 1947, the United States' intelligence services have supported the country's leaders by obtaining and analyzing

---

[102] Zoe Haver, Private Eyes: China's Embrace of Open-Source Military Intelligence, Recorded Future at 1 (2023).

[103] Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, U.S. Senate Select Committee on Intelligence (2020).

[104] Claire Allbright, A Russian Facebook Page Organized a Protest in Texas. A Different Russian Page Launched the Counterprotest, The Texas Tribune (2017).

adversaries' secrets, offering a decision advantage to U.S. policymakers. Today's IC has exceptional tradecraft and capacity in the world of classified intelligence but is grappling with how to stay atop of the vast amounts of openly-available information that is growing exponentially each year, and largely being produced outside the scope of what the U.S. Government collects and analyzes. 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.[105] Doing so is also vital to protect the U.S. Government's activities and sensitive secrets that are increasingly exposed or discoverable in an open-source ecosystem.

The IC In Danger of Falling Behind

In addition to the Open Source Enterprise at CIA, which carries on the legacy of open source collection from its earliest days as the Foreign Broadcast Monitoring Service established in 1941,[106] there are many other open source entities throughout the national security community. These open source units can and do make remarkable contributions to the mission by coupling open insights with classified data, but IC agencies face many barriers when trying to tap into the flow of open source data and analytics. Most exclusively serve the missions of and are bound by the authorities of their organizations; they generally are staffed by those with security clearances and deep substantive expertise in a topic or part of the world. This specialized expertise is essential: a China military expert at the DIA has different focus areas and authorities than a China intelligence analyst expert at the Federal Bureau of Investigation (FBI) or one who supports CIA targeting. But as a consequence, these IC units do not "live" in the open source space. They tend to focus most of their energies on classified intelligence priorities, leaving little time for unclassified intelligence analysis. This secrets-centric foundation has enabled U.S. success for decades and has created an understandable bias towards and familiarity with secret information. The workforce can also distrust technical approaches because it understands the potential for abuse and does not fully understand how to use technology to sift through open data. With busy professionals fully employed managing their classified data queues, it is exceptionally challenging to develop the needed depth expertise across the breadth of open source datasets and tools that the world produces at the speed of the internet.

More importantly, the IC's open source units do not have access to the full spectrum of private sector data, analytics, and business expertise across the myriad of disciplines required for companies to grow and function. The lack of access is partly driven by how limited sources are allocated (the IC has many times more imagery analysts than OSINT analysts, for example) and by internally-driven security and counterintelligence restrictions. While open systems' technology and data move quickly and at volume, the IC's systems are hampered by lengthy contract

[105] The IC OSINT Strategy 2024-2026, Office of the Director of National Intelligence (2024).
[106] Steven Aftergood, Open Source Center (OSC) Becomes Open Source Enterprise, Federation of American Scientists (2015).

processes and necessarily cumbersome security protocols. Once established, getting to the open data or finding the right tool is not straightforward as new companies with interesting data or tools are constantly being created and well-known companies' capabilities can atrophy or become less relevant as the mission changes. While small units engage with industry, there is no clearinghouse or front door scales to the breadth and volume of capability that could be of value to the government. Surveying them all and keeping current on their capabilities would be the job of dozens of people. Even when a vendor or vendors are selected, moreover, getting them on contract and into the system can take many months.

Meanwhile, 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 U.S. Government concern, ranging from human trafficking networks, Chinese presence in the US, ghost ships hiding their global positioning systems (GPS) signals, and nuclear proliferation, among a few.[107] They have found tools and strategies to absorb and analyze new data and push out products at the speed with which the data becomes available to serve their customers/audiences. Companies like Starbucks, Disney, and Dow Chemical all have open-source units to help them understand the market, protect their people and facilities, and secure their brands.[108] These companies make billion-dollar decisions based on their teams' analyses, and their employees advance their skills, tools, and tradecraft at a speed not possible with the acquisition and security brakes in place by the government.

In addition, the ease of accessing the world's data means that anyone with a computer, smartphone, access to the internet, and persistence can expose nation-state secrets[109]. Nearly anyone can become an open source investigator, and thousands have become part of the crowd-sourcing networks that publish their findings online. While their work can be uneven, it also can be exceptional.

Little of the above comes as a surprise to national security professionals who operate in the open source space. Over the last decade, the open source problem has been the subject of many data calls, conferences, academic papers and op-eds, even as this open source ecosystem has exploded into volumes rivaling that collected by the U.S. Government.[110] Finding a way to understand its insights at the speed of mission has become even more critical. Some senior

[107] See e.g., Zero Trafficking (last accessed 2024); Strider Technologies (last accessed 2024; Whitespace (last accessed 2024); John Warrick, China is Building More Than 100 New Missile Silos in its Western Desert, Analysts Say, Washington Post (2022).
[108] Why You Should Care About Open-Source Agronomy, Starbucks (2022); Open Source, Disney (last accessed 2024); Ralph Lauren and Dow Open-Source New Process to Transform How The Fashion Industry Dyes Cotton, Dow (2021).
[109] Elliot Higgins, We are Bellingcat: An Intelligence Agency for the People, Bloomsbury Publishing (2021).
[110] Michael Glassman & Min Ju Kang, Intelligence in The Internet Age, Computers in Human Behavior (2012); Heather Williams & Illan Blum, Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise, RAND Corporation (2018); Chris Rassmussen, Avoiding the Secrecy Trap In Open Source Intelligence, The Cipher Brief (2023).

national security officials believe the way forward remains within the community's current construct. After so many studies, an all-encompassing solution has not yet been implemented. However, ODNI recently created a new Open Source Executive position and articulated a set of guidelines on the IC's use of commercially-available data that may offer more progress.[111]

An Interim Approach: Creating A Public-Private Partnership for Open Source

Several national security experts believe it is essential that the U.S. Government establish a new Open Source entity to address the shortcomings of the existing model and whose sole mission would be to harness the power of openly- and commercially-available data to ensure decision advantages.[112] This new entity would be responsible for collecting and acquiring, analyzing, and sharing open-source data and analysis across the IC and with policy agencies.[113]

Since establishing a new agency, inside or outside the IC, will require strong support from the White House and Congress, and will likely take time to properly resource, it may be some time before such an outcome is accomplished. But in the meantime, the urgent need to expand the IC's open source capabilities cannot wait. As a bridge to a time when the Open Source Agency is fully established, the U.S. Government could create a new national security-focused non-profit organization – akin to IQT – to enable rapid capacity improvement for all IC agencies. Hundreds of commercial companies already produce valuable data, tools, and insights in the open-source space. A non-profit organization could bring their products and services together in a vetted consortium guided by IC priorities and tradecraft standards, allowing the government to benefit from their capabilities without being weighed down by the administrative challenges of identifying, contracting, integrating, and maintaining them. The IC could direct the work of this consortium with minimal initial staffing, and the new entity could be created quickly, within a fiscal year, were Congress to direct appropriated IC budget funds for the effort and the IC establish its role and mission.

Undertaking this program in a new 501(c)3 organization with a similar framework could address pressing challenges. Notionally referred to here as Open Source Intel (Os-N-Tel), its focus would be on enabling the IC's mission by acting as a clearinghouse to identify and provide access to the world's data through a consortium of companies offering the best data sources, tools, and data technology. The IC already buys a tremendous amount of data and has many tools to exploit it. However, thousands of entities – companies, non-profits, and academic institutions could make

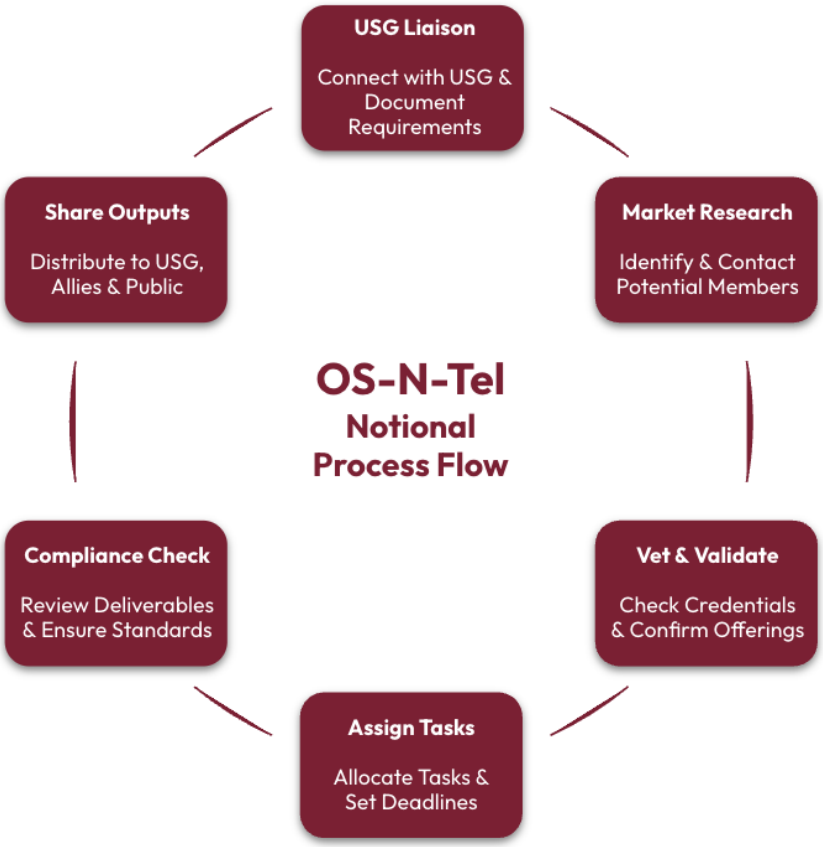
[111] The IC OSINT Strategy 2024-2026, Office of the Director of National Intelligence (2024).

[112] Jeanne Meserve & Michael Morell, Episode 31: Michael Morell on the CIA's Use of Emerging Technologies, Special Competitive Studies Project (2023).

[113] SCSP included this recommendation, along with three other constructs in its 2022 Intelligence Interim Panel Report. Intelligence in An Age of Data-Driven Competition, Special Competitive Studies Project (2022).

vital contributions to the mission. Os-N-Tel could take on the heavy research, contracting, and data management challenges currently carried by government officers, including identifying and vetting these companies, getting them on contract, and pushing their capabilities and insights to government-directed mission needs. One of China's most effective programs against us is that they don't have a "not invented here" approach to technology and data. They will steal it, buy it, or invest in companies that produce it to create a competitive advantage for Beijing without having to spend time or money on the research and development. The IC can create its own competitive advantage by leveraging a consortium of private sector capabilities to gain speed to insight (without, of course, replicating China's nefarious activities).

Additionally, the data economy and its exploitation by adversaries create new threats that entities outside government are sometimes best positioned to see, from supply chain issues to AI-enhanced biotech challenges. Increasing insights from a consortium of national security-related companies, venture capital-backed and Fortune 500 companies, academia, non-profits, and open-source investigating organizations worldwide could be transformative for the mission. Os-N-Tel could offer a single place online to make available the analyses, reports, and other insights already published by these entities.



As with IQT, the government would guide Os-N-Tel directionally through its requirements, and the organization would consist of a small team with deep expertise in data, open source information, privacy and civil liberties, and the private sector. Together with government and industry partners, questions related to contracts, requirements, fulfillment, and payment, as well as a myriad of other important systems and process decisions would need to be made. With focus, it is doable in a relatively short amount of time.

With much about the new data economy still unformed, the IC could further task Os-N-Tel to drive progress on establishing best practices in many areas, such as:

- Sharing tradecraft standards between the IC and the private sector, expanding the interconnectivity of insights to benefit both.

- Leveraging more bulk open data at scale, using several AI/ML tools. Expanding the IC's resources and training on maintaining analytic objectivity and avoiding bias to include private-sector collectors, technologies, and analytic tools would be in the IC's long-term interests.

- Standardizing IC approaches to data rights, pricing, and data pedigree, making available a collaborative space for users to try out vetted new tools or technologies, including large language models and GenAI.

- Serving as an additional mechanism for sharing information with private-sector national security decision makers and in service of the public good, including a discussion of privacy, civil liberties, and how U.S. adversaries already use Americans' data.

National security leaders will decide how much of the enormous open-source ecosystem they want to assume responsibility for understanding. Os-N-Tel could support their success by applying deep private-sector and open-systems expertise to create a needed ecosystem that frees government employees to focus on higher-order work in their areas of expertise. Creating this expansive capability to draw insights from the world's data in an era of heightened global uncertainty will not be easy. However, data, tools, technology, and insights available now in the public domain – but not in government hands – could help close critical knowledge gaps about the country's most significant challenges; understanding and operationalizing the information is crucial to the success of the national security community and the nation.

Enabling a More Proactive U.S. Strategic Communications Posture

The information domain is rapidly evolving, driven by technological change, the displacement of traditional mass media platforms, and more focused efforts by anti-democratic regimes. These changes make the strategic consequence of malign behavior in the information domain more consequential now than it was in the past. Compounding and even supercharging the changes brought on by the Internet is the emergence, more recently, of new technologies like generative artificial intelligence. GenAI can significantly alter the speed of creation and quantity of information in the world, including inaccurate and deliberately false information.[114] The newest wave of GenAI models can be used to create synthetic media like deepfakes that are undetectable to the human eye.[115] And these new capabilities enable aggressors to microtarget individual citizens with persuasive false and misleading information. The potential challenge in all of this is that trends from the Internet and emerging technologies come together to form an information domain in which there is an ever-increasing amount of information, expanding threats of disinformation and vectors of influence, and very little public trust in such information or ability to separate truth from fiction – or what some experts call the "Information Apocalypse."[116]

How the U.S. Government deals with strategic communications, however, has not kept pace with this changed information landscape. Responsibility for strategic communications remains divided between several different departments and agencies. The Department of State has generally held the leadership role for strategic communications external to the United States, while the Department of Defense and IC have played specialized roles in the information domain. The State Department's Global Engagement Center leads U.S. Government efforts around countering disinformation,[117] with a heavy focus on publishing reports regarding Russian operations. Other efforts in the information domain include the ODNI's Foreign Malign Influence Center, which integrates and leads U.S. intelligence efforts around countering foreign influence.[118] This stands in stark contrast to how other nations – including China, Russia, and many U.S. allies such as Israel and the United Arab Emirates – are prioritizing information operations.

[114] See Josh A. Goldstein, et al., Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations, OpenAI (2023).
[115] Katerina Sedova, et al., AI and the Future of Disinformation Campaigns Part 1:The RICHDATA Framework, Center for Security and Emerging Technology (2021); Katerina Sedova, et al., AI and the Future of Disinformation Campaigns Part 2: A Threat Model, Center for Security and Emerging Technology (2021); Todd C. Helmus, Artificial Intelligence, Deepfakes, and Disinformation, RAND Corporation (2022).
[116] Mari K. Eder, The Information Apocalypse… Is Already Here, U.S. Army War College War Room (2018).
[117] Mission & Vision, Global Engagement Center, U.S. Department of State (last accessed 2024).
[118] Organization: Foreign Malign Influence Center, Office of the Director of National Intelligence (last accessed 2024).

Rival Approaches: China and Russia

The challenges from China in the information domain are a useful point of departure for outlining the range of areas in which the IC could contribute to U.S. positional advantage in the information domain. For example, in his speeches and diplomatic engagements, Xi Jinping has emphasized the need to reform global governance as part of Beijing's goal to become the world leader and achieve global recognition of what it calls "Socialism with Chinese Characteristics" as a legitimate alternative to democratic values.[119] The PRC's Global Development Initiative and Global Security Initiative are further intended to disrupt two foundational elements of the international system: (1) the normative linkage between political liberalization and development and (2) the U.S. alliance system. In addition, the PRC has pursued the "One Belt, One Road" and the Digital Silk Road initiatives as the physical manifestation of Beijing's interest in rewiring the world in ways that reinforce PRC centrality.[120] To accomplish its objectives, the PRC has sought to undermine the international organizations from the United Nations to the World Bank to international standards setting bodies.

These PRC initiatives aim, in part, to control the means of communication – both the content creators and the infrastructure through which content is disseminated – and then shape the information environment through propaganda and censorship. How Beijing pushes this forward varies across countries, based on what footholds different PRC actors are able to establish. In some cases, like Ecuador, the relationship begins with the cultivation of national leadership, which led to the deployment of PRC technology.[121] In others, like the Solomon Islands, infrastructure investments planted the seeds for Beijing's influence from which larger political change grew, including democratic backsliding, shifting recognition from Taipei to Beijing, and denying U.S. access to port facilities.[122] As PRC influence increases, the local information environment often becomes more closed off, because Beijing provides training in human and technical propaganda and censorship techniques.

Meanwhile, for decades, Russia's operations have focused on contaminating the information domain in an effort to make it more difficult to know what is real and what is not and to undermine cohesion between nations and within their borders.[123] These efforts range from overt

[119] Daniel Tobin, How Xi Jinping's 'New Era' Should Have Ended U.S. Debate on Beijing's Ambitions, Center for Strategic and International Studies (2020).
[120] Elizabeth Economy, Xi Jinping's New World Order, Foreign Affairs (2021); Samantha Hoffman & Nathan Atrill, Mapping China's Tech Giants: Supply Chains and the Global Data Collection Ecosystem, Australian Strategic Policy Institute (2021).
[121] Paul Mozur, et al., Made in China, Exported to the World: The Surveillance State, New York Times (2019).
[122] Cleo Paskal, Right to Vote Being Snatched from Solomon Islanders by PRC-backed PM, Sunday Guardian (2022); Cleo Paskal, The U.S. is Blocked From Ports in PRC-Influenced Solomons, Vanuatu, Sunday Guardian (2023); Damien Cave, China's Mad Dash Into a Strategic Island Nation Breeds Resentment, New York Times (2023); Bemobile Enlists Huawei to Boost Networks in Solomon Islands, PNG, Comms Update (2014).
[123] Richard Schultz & Roy Godson, Dezinformatsia: Active Measures in Soviet Strategy, Pergamon-Brassey's (1984); Kevin McCauley, Russian Influence Campaigns Against the West: From the Cold War to Putin, CreateSpace Independent Publishing Platform (2016).

propaganda to covert influence, and occur both from inside and outside Russia, all with the purpose of creating and exploiting fissures in target audiences for Moscow's benefit. The pillars of this system are official government communications, state-funded global messaging, cultivation of proxy sources, weaponization of social media, and cyber-enabled disinformation.[124] Recent examples include encouraging the rise of far right parties across Europe,[125] spreading rumors about U.S. biological weapons labs in Ukraine,[126] and emphasizing how Moscow's critics were insane, Russophobic, and hysterical.[127] Moreover, late 2023 reporting indicates that Russia has been involved in physical and digital efforts to influence elections around the world ahead of 2024, including in unnamed South American and European countries.[128] Because the goal of these efforts is disruption and confusion, the propagated narratives do not need to be consistent (and are often contradictory).[129]

Limitations

The U.S. Government's current approach to the information domain tends to be somewhat reactive and fragmented across multiple agencies, which in turn makes it particularly challenging for the intelligence community to provide its support. The relevant departments and agencies tend to be focused on their departmental priorities, which are not always oriented toward national advantage. Challenging features of the U.S. Government's information efforts include:

- **Balkanized Efforts.** Compared to its adversaries, the United States has largely disaggregated its information efforts. The U.S. Government currently has at least seven departments and agencies assigned to handle various subsets of the information mission,[130] though some have argued that U.S. strategic communications and public diplomacy are fragmented among 14 agencies and 48 commissions.[131] These entities also tend to have relatively narrow mandates. They might be focused on a specific objective rather than being a resource for their department or the broader U.S. Government.

[124] GEC Special Report: Russia's Pillars of Disinformation and Propaganda, U.S. Department of State at 8 (2022).
[125] Gabriel Gatehouse, Marine Le Pen: Who is Funding France's Far Right?, BBC (2017); Paul Kirby, German Elections: Why This is a Turning Point, BBC (2017); Matt Bradley, Europe's Far-Right Enjoys Backing from Russia's Putin, NBC (2017).
[126] Bill Chappell & Odette Yousef, How the False Russian Biolab Story Came to Circulate Among the U.S. Far Right, NPR (2022).
[127] #PutinAtWar: How Russia Weaponized 'Russophobia', DFR Lab (2018).
[128] Tim Starks & David DiMolfetta, Russia is Undermining Election Integrity in Democracies, Cable Warns, The Washington Post (2023).
[129] After the 2018 Russian poisoning of defector Sergei Skripal, Russian outlets put out more than 130 competing and contradictory narratives about what might have occurred to sow doubt about Moscow's culpability. See Gordon Ramsy & Sam Robertshaw, Weaponising News: RT, Sputnik, and Targeted Disinformation, King's College London Policy Institute at 6 (2018).
[130] Entities include, but are not limited to: Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency and Department of Defense's CyberCommand, Department of State's Global Engagement Center, Federal Bureau of Investigation's Foreign Influence Task Force, Office of the Director of National Intelligence's Foreign Malign Influence Center, U.S. Agency for International Development, and the U.S. Agency for Global Media.
[131] Robert M. Gates, The U.S. Needs to Relearn How to Tell Its Story to the World, The Washington Post (2023).

- **Reactive Approaches.** U.S. Government activities in the information domain generally tend to be reactive and defensive in nature. For example, ODNI's Foreign Malign Influence Center (originally proposed to be the Foreign Malign Influence Response Center) is tasked with "countering the enduring threat" of hostile foreign influence, to include (but not limited to) exposing foreign operations and efforts to interfere with elections.[132] Other, non-IC efforts that previously served strategic purposes, such as the Fulbright Program and other forms of professional exchange, are now viewed primarily as educational or cultural exchanges.[133] Even U.S. Government-funded media broadcasts, like those under the aegis of the U.S. Agency for Global Media, are defined as a reaction to the actions of other actors abroad. For example, Radio Free Europe/Radio Liberty's mission is "providing accurate, uncensored news and open debate in countries where a free press is threatened and disinformation is pervasive."[134]

- **Unclear Purpose.** The U.S. Government's vision for information advantage is not always clear. First, the U.S. Government does not appear to have a unified and purposeful strategy for the information domain. Similarly, there does not appear to be a unified concept for how such a goal of advantage in the information domain would translate into specific activities by its various departments and agencies. Second, it is not always clear what department or agency has the lead on a given issue (except for covert influence). And, third, the authorities and responsibilities of various departments and agencies, including members of the IC, in this space are not all well-known or publicly accessible, making it difficult to direct recommendations.

The Proper Role for the IC

Countering Chinese and Russian disinformation with effective U.S. strategic communications is not solely the IC's responsibility; indeed it is primarily the responsibility of policy agencies and law enforcement. However, the IC can – and should – put a higher priority on supporting policy efforts, particularly in these areas:

[132] Organization – Foreign Malign Influence Center, Office of the Director of National Intelligence (last accessed 2024).
[133] What is the Fulbright U.S. Student Program, Fulbright (last accessed 2024).
[134] Radio Free Europe/Radio Liberty, U.S. Agency for Global Media (last accessed 2024).

- **Understanding Emerging Platforms and Mediums of Communications.** The IC must establish and continuously update a baseline understanding of the primary foreign platforms and mediums of communication that contribute to today's information domain. Functional specialists in technology and software should develop a sufficient level of understanding of these platforms to exploit or disrupt them in support of U.S. policy objectives. Meanwhile, regional experts should identify local foreign platforms of communication and help inform content development.

- **Mapping the Adversarial Information Order of Battle.** The IC needs to track the organizations, individuals, resources, and messaging the PRC, Russia, and other adversaries are using at home and abroad. This baseline information also should include exchange programs, media training, and other forms of people-to-people engagement. Such work should be the responsibility of the regional analytic offices.

- **Disrupting Adversary Information Operations.** In addition to the information order of battle in general, the IC should particularly track information operations by foreign adversaries. The purpose here is not just to generate insights, but crucially, to identify vulnerabilities for U.S. policymakers to direct disruptive efforts. Regional specialists for both rival countries and targeted countries would be best suited to lead these efforts, with functional experts providing analysis of technological vulnerabilities and tech-enabled options to disrupt them.

- **Modernizing Covert Influence Tools to Support U.S. Policy.** The IC should also use its infrastructure for covert influence capabilities to support U.S. strategic communication efforts abroad. The IC ought to continuously update and refine its approach, while avoiding getting involved in disinformation.[135]

- **Assisting Policy Agencies Measure the Effectiveness of Strategic Communications.** The IC also should be helping decision makers understand how foreign audiences and U.S. rivals are responding to U.S. initiatives and policies. Some signs of success or failure are likely to be visible, such as whether a contract for seaport management is signed. Others, however, may require tracking financial transactions, audience surveys, or other actions by local actors. Modern software and connectivity enables more targeted and more continuous surveys on a global scale.

Recommendations

The IC can create the infrastructure and policies necessary to facilitate a broader exchange of information between IC agencies and state and local authorities, federal civilian regulatory agencies, academia, and the private sector. This will help to enhance national competitiveness with and resilience against enduring and emerging threats.

Clarify existing authorities among the components of the IC and U.S. Government as a whole that have roles in strategic communications. The DNI should review authorities for strategic communications across IC elements and the interagency in coordination with the NSC. The goal should be identifying opportunities for collaboration and complementary efforts between the IC, State Department, DoD, USAID, and other agencies with public communications roles. Any gaps, redundancies, or unclear lanes of responsibility should be clarified.

Build expertise on foreign malign information operations and capabilities. Additional collection and analytic resources should be focused on understanding communications platforms and channels that underpin today's information environment, assisting in uncovering and monitoring adversary information operations, capturing information, generating insights, issuing timely warning and opportunity analysis, engaging in covert efforts, tracking foreign audiences and sentiments, and providing operational support to and measuring effectiveness of strategic communications.

- **Enable Automated Sentiment Analysis Abroad.** ODNI and IC agencies should develop infrastructure for automated, continuous sentiment analysis of foreign populations and audiences. This will leverage AI tools to gauge public opinion in adversaries and allied

[135] Josh Baughman & Peter W. Singer, China Gears Up for Cognitive Warfare, Defense One (2023).

nations to inform operations and assessments. Successful development and integration of such automated sentiment analytics is estimated to cost $200 million.

- **Counter disinformation and foreign malign influence at the source.** To better counter adversarial operations, particularly as more sophisticated AI tools come into play, the IC should focus on acquiring technological capabilities to quickly identify AI-generated disinformation by our adversaries. Just as the IC became the authority for analyzing and authenticating the audio recordings of the leadership of al-Qaeda and the Islamic State terrorist organizations in the aftermath of 9/11, the DNI should establish intelligence community standards and capabilities for identifying and "prebunking" disinformation.[136] ODNI should acquire AI tools to detect synthetic disinformation content. In addition, the FBI and Department of Homeland Security (DHS), supported by the IC, should establish a public information sharing program to warn social media and other appropriate technology companies, local governments, and citizens of ongoing disinformation campaigns by adversaries that could cause harm.

Prioritize Going on the Offense. Engaging in covert influence is ultimately a presidential decision. The IC, however, does have responsibility for ensuring that it maintains robust capabilities to act if the President decides to do so. Those capabilities need to enable the United States to engage in two key terrains – first, inside the adversary's information space, and, second, in undermining the adversary's ability to project malign influence abroad. The target of such operations would be adversarial actors and populations within the identified key terrains.

- **Maintain and enhance the capacity to operate in closed foreign information environments.** The DNI should work closely with IC leaders, especially those Title 50 Agencies focused on the collection of foreign intelligence more specifically, to ensure that it has the capacity to operate inside heavily controlled information environments, like Iran, North Korea, Russia, and, crucially, China. This means having the access to undermine host-nation firewalls, both partially and entirely, and having the capability to deliver targeted content in local platforms in peacetime or flood the information space in the event of a crisis or contingency. While heavily censored environments provide a challenge to building IC operations, the need for such capacities remains. The exact format for achieving these ends should be tailored to relevant Title 50 entities, but could be appraised setting yearly benchmarks and assessments where viable.

[136] Prebunking is the process of early disclosures and pre-emptive efforts to debunk information, sources, and tactics. For more on prebunking, see Laura Garcia & Tommy Shane, A Guide to Prebunking: A Promising Way to Inoculate Against Misinformation, First Draft (2021); Jon Roozenbeel, et al., Prebunking Interventions Based on "Inoculation" Theory Can Reduce Susceptibility to Misinformation Across Cultures, Harvard Kennedy School Misinformation Review (2020).

- **Develop the capacity to disrupt adversaries' information platforms and messaging abroad.** Both China and Russia export tools to control information environments, which in turn reinforces democratic backsliding and autocratic control.[137] The DNI should be provided the authority and appropriate funding to establish a program at CIA and NSA to continuously gather intelligence on authoritarian information control technologies to inform development of countermeasures. The CIA and NSA should build capacities to circumvent internet censorship controls in closed societies to deliver information and enable dissent, as was done for Polish Solidarity.[138] Technical abilities to disrupt adversaries' propaganda platforms abroad, whether on or offline, should also be developed. Furthermore, such disruption need not be purely technical. For example, the elite capture and corruption that precedes many Chinese infrastructure projects overseas can be targeted to counter the capabilities that would be put in place through data storage and cloud computing centers, telecommunications projects, and other digital infrastructure.

Build incentives to attract talent from fields that benefit a new strategic communications posture. The new information domain, especially the tools of the new information domain, require additional talent and skill sets – ranging from anthropologist and sociologists, to network analysts, to data scientists, to generative AI engineers. In addition to these functional and technological skills, the IC should aim to increase regional and country-specific expertise.

- **Expand staffing in key expertise areas through targeted recruiting and funding.** To build expertise in strategic communications, the DNI should set 5 percent annual growth targets for staffing levels at IC agencies in relevant skill areas including social media analytics, network mapping, regional cultures, and influence operations. Agencies should recruit personnel with specialized backgrounds through fellowships and by prioritizing technical disciplines identified as critical by the Office of Science and Technology Policy. Expanded hiring likely requires additional funding. Agencies should report annually on staffing growth in key expertise areas to enable oversight.

- **Develop and retain critical skills that advance support for 21st Century strategic communications through incentives and training programs.** Specifically, IC agency human capital leads should streamline the process of private-public rotations, enable professional development training and certification up to 90 days annually (for critical technologies identified by OSTP), and incentivize sustaining abilities in advanced technologies like AI and foreign languages.[139] Ensuring expanded access to the above

[137] Paul Mozur, et al., Made in China, Exported to the World: The Surveillance State, New York Times (2019).
[138] Seth Jones, A Covert Action: Reagan, the CIA, and the Cold War Struggle in Poland, W. W. Norton & Company (2018).
[139] Language Opportunities – Foreign Language Incentive Program, Central Intelligence Agency (last accessed 2024); Joe Pappalardo, The Air Force Will Treat Computer Coding Like a Foreign Language, Popular Mechanics (2018).

programs likely requires Congress to authorize additional professional development and skill incentive programs, and appropriate necessary funds. Agencies should track program usage and assess impact on retaining talent.

APPENDIX A

Recommended Actions

Theme	Recommendation	Stakeholder(s)	Description	Actions
Seize the GenAI Moment	Publish ODNI guidance on the use of AI across the IC.	DNI	The new IC AI Council should publish an Intelligence Community Directive (ICD) that defines acceptable uses for generative AI.	Policy and Oversight
Seize the GenAI Moment	Expedite processes for talent exchange programs	DNI	The DNI should implement talent exchange programs for temporary assignments of IC and private sector AI experts.	Talent Development & Exchange
Seize the GenAI Moment	Increase collection and analysis on foreign AI capabilities	DNI	The DNI should increase intelligence collection and all-source analysis on foreign development and potential uses of AI tools.	Assessments & Reviews
Seize the GenAI Moment	Develop doctrine for human-AI teaming	DNI	The DNI should develop formal doctrine on combining human-machine teaming for intelligence analysis.	Technology & Tradecraft
Reimagine IC Partnerships	Appoint a Deputy DNI for Intelligence Partnerships	DNI, Congress	This position would coordinate intelligence sharing, guide data access policies, and manage key partnerships with allies.	Institutions & Positions
Reimagine IC Partnerships	Institute regular reviews of partner contributions	DNI, Deputy DNI, IC Heads, Congress, Allies	The DNI should regularly review allied intelligence contributions and provide capacity building. Congress should authorize ending unproductive relationships.	Policy & Oversight
Reimagine IC Partnerships	Expand secure communications capabilities	IC CDO, IC CDOC, Allies, Industry	The IC CIO should scale up SVTC capabilities and user-friendly interfaces for multilateral engagements.	Technology & Tradecraft
Reimagine IC Partnerships	Build digital platforms for collaboration	DNI, IC CDO, IC CDOC, Allies, Industry	The DNI and IC technical leads should develop virtual platforms for allies to jointly assess threats and conduct collaborative analysis.	Technology & Tradecraft
Reimagine IC Partnerships	Incentivize public-private partnerships on AI	DNI, Congress	DNI should incentivize partnerships focused on (1) transitioning commercial AI capabilities to operations and (2) building out the IC's network with non-state entities. Congress should consider appropriate budget increases to ensure partnership(s) success.	Partnerships & Collaborations
Leveraging Open Source	Create a public-private OSINT consortium	DNI, IQT, Economic Security & Financial Intel Executive, Industry	Expand IQT or create a 501(c)3 "Open Source Intelligence" organization for public-private partnerships to improve IC access to open source data.	Institutions & Positions

Leveraging Open Source	Increase use of open source intelligence	DNI, OSINT Executive	The DNI should empower the OSINT Executive to increase IC use of open source by promoting OSINT tradecraft and expanding IC access to OSINT data and analytics tools.	Technology & Tradecraft
Enable U.S. Strategic Communications	Acquire advanced commercial information and communications technologies	DNI, IC CDO, IC CDOC, IC agencies	IC elements should procure subscriptions, software, machine learning models, and other innovations from the private sector.	Technology Adoption
Enable U.S. Strategic Communications	Build expertise in emerging information and communications technologies	DO, DIA, NSA	Agencies should substantially increase staffing and expertise in influence operations, strategic communications, and related areas.	Talent Development
Enable U.S. Strategic Communications	Set standards for countering foreign malign influence	DNI, FBI, DHS	The DNI should set standards for identifying and rebutting disinformation. The FBI/DHS should warn companies and the public.	Policies & Oversight
Enable U.S. Strategic Communications	Recruit talent to bridge expertise gaps	DNI, IC agencies	Agencies should recruit staff with skills in areas like social media analytics, AI engineering, and adversarial thinking.	Talent Development