SPECIAL COMPETITIVE STUDIES PROJECT

INTELLIGENCE

Interim Panel Report

October 2022

Contributors

SCSP LEADERSHIP

Dr. Eric Schmidt, Chair
Ylli Bajraktari, President & CEO

BOARD OF ADVISORS

Michèle Flournoy
Dr. Nadia Schadlow
William "Mac" Thornberry III
Robert O. Work

INTELLIGENCE PANEL

Peter Mattis, Director
Meaghan Waff, Associate Director
Katherine Kurata, Associate Director
Sinclair Im, Research Assistant
Brian Wiltse, Research Assistant
Ylber Bajraktari, Senior Policy Advisor

INTELLIGENCE ADVISORS

Rodney Faraon
Glenn Gaffney
Dawn Meyerriecks
Dean Souleles
Dr. Amy Zegart

The Intelligence Panel Interim Panel Report (IPR) is the second of six interim reports from the overall work that the Special Competitive Studies Project (SCSP) conducted over the past year and that was summarized in our Mid-Decade Challenges to National Competitiveness report published on September 12, 2022. This report benefited greatly from insights and expertise by a number of individuals to whom we are deeply grateful. It aims to reflect many, though not all, of those insights. It was prepared by the SCSP staff and, as such, it is not a consensus document of all the experts who assisted.

INTELLIGENCE PANEL INTERIM PANEL REPORT

Intelligence in An Age of Data-Driven Competition

The mid-decade challenge for the U.S. Intelligence Community (IC) is winning the accelerating race for actionable insight to enable U.S. statecraft in a more information-rich and geopolitically competitive world.

For the first time since the Cold War, the United States faces a rival – the People's Republic of China (PRC) – that is competing globally across the economic, political, social, information, and military domains to reshape, if not dominate, the international order. As the most recent National Security Strategy of the United States put it, "The PRC is the only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it."[1] For the IC, this rivalry will govern not only what U.S. leaders ask of it, but also how it must evolve to meet this challenge. In a rivalry with a technological and economic near-peer, and with technology as a key battleground of the competition, providing insight into our adversaries' emerging technologies and the organizations that field them is as important as understanding the traditional political and military institutions of a state.[2]

In addition to the geopolitical context, the exponential increase in data generation and in surveillance, monitoring, and collection technologies is creating avalanches of data. Like all U.S. Government organizations, the IC faces challenges to collect, process, and exploit all this data. Moreover, once government-unique capabilities, like geospatial[3] and signals intelligence,[4] have been commercialized. Private companies can now provide tailored analytic products to U.S. Government consumers on breaking events, sometimes ahead of the IC, in part because they are better positioned or equipped to use AI and other emerging technologies. These companies can also select contracts or exploit opportunities that specifically showcase their comparative strengths.[5] Meanwhile, the demand of policymakers for insight

[1] National Security Strategy of the United States of America, The White House at 23 (2022).
[2] Corin Stone, A Roadmap for AI in the IC, The Cipher Brief (2021); Amy Zegart, American Spy Agencies Are Struggling in the Age of Data, Wired (2022); Corin Stone, Artificial Intelligence in the Intelligence Community: The Tangled Web of Budget & Acquisition, Just Security (2021).
[3] In 2021, the IC designed a Commercial Space Council to identify how intelligence deliveries that rely on commercial satellites can be accelerated. DNI John Ratcliffe's Remarks at the Eighth Meeting of the National Space Council, Office of the Director of National Intelligence (2020); Todd Harrison & Matthew Strohmeyer, Commercial Space Remote Sensing and Its Role in National Security, Center for Strategic and International Studies (2022).
[4] Cortney Weinbaum, et al., SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain, RAND Corporation (2017).
[5] Elizabeth Leyne & Yvette Nonté, Is the Intelligence Community Staying Ahead of the Digital Curve? A Survey of its Highest-level Customers and Leaders on the Challenges and Opportunities Ahead, Belfer Center for Science and International Affairs (2021).

across an ever-broader array of issues may lead them to turn more frequently to the private sector, or to try and find the data they need on their own in the public domain.

U.S. intelligence is capable of rising to the occasion and delivering on the seemingly impossible and the once-unthinkable. The IC was able to successfully warn the White House, Ukraine, and its allies of the Russian invasion months before its actual occurrence.[6] The early and rapid declassification of this intelligence allowed U.S. policymakers to counter Russian disinformation credibly, undermine the possibility of false flag operations, discredit the Kremlin narrative, and strengthen the allied response.[7] This and similar efforts are possible because the IC – along with its U.S. Government partners – operate the world's largest constellation of human and machine sensors located anywhere from undersea to outer space.

IC leaders understand many of the challenges of this new era of techno-economic competition. They were among the first in the U.S. Government to experiment with AI,[8] initiating numerous AI projects,[9] organizational shifts,[10] and new efforts to capture data outside government channels.[11] IC leaders recognize that once-unique U.S. collection capabilities are now known and used by foreign intelligence services.[12] The PRC and other hostile actors are exploiting the opportunities afforded by ubiquitous technical surveillance to become global counterintelligence threats.[13] Moreover, as the PRC builds out digital infrastructure globally, U.S. intelligence will more frequently operate where Beijing can apply its own technology-enabled tools, including AI and biotechnology, to expose U.S. operations.[14] The IC leadership's understanding and attempts to address these challenges, however, have not yet translated into sustainable, community-wide change.

In this new context, the IC's ability to provide competitive advantage to U.S. policymakers will hinge on whether it can integrate and master emerging technologies, particularly AI, and fuse more diverse sources of information across all domains. The IC's ability to unlock new insights in support of U.S. statecraft will require action in the following areas:

---

[6] Shane Harris & Paul Sonne, Russia Planning Massive Military Offensive Against Ukraine Involving 175,000 Troops, U.S. Intelligence Warns, The Washington Post (2021).

[7] Felicia Schwartz & Demetri Sevastopulo, A Real Stroke of Genius': US Leads Efforts to Publicise Ukraine Intelligence, Financial Times (2022); Press Briefing by Press Secretary Karine Jean-Pierre and NSC Coordinator for Strategic Communications John Kirby, The White House (2022).

[8] Maxime Fischer-Zernin, Narrative Science: The CIA is Investing in Artificial Intelligence That Actually Works, MIC (2013).

[9] The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines, Office of the Director of National Intelligence (2019); DIA's "MARS" Initiative Reaches Another Key Milestone, Defense Intelligence Agency Public Affairs (2021); NGA Releases New Data Strategy to Navigate Digital, GEOINT Revolution, National Geospatial-Intelligence Agency (2021); Sarah Scoles, Meet the US's Spy System of the Future — It's Sentient, The Verge (2019); Mark Pomerleau, NSA's Cybersecurity Directorate Looks to Scale Up This Year, C4ISRNET (2022); Patrick Tucker, What the CIA's Tech Director Wants from AI, Defense One (2017).

[10] See, e.g., Organization: Directorate of Digital Innovation, Central Intelligence Agency (last accessed 2022); Quint Forgey & Daniel Lippman, CIA Launches New China-Focused Unit, Politico (2021).

[11] Steven Aftergood, Open Source Center (OSC) becomes Open Source Enterprise (OSE), Federation of American Scientists (2015); Justin Doubleday, Spy Agencies Look to Standardize Use of Open Source Intelligence, Federal News Network (2022); Justin Doubleday, State Department Intelligence Arm to Set Up Open Source Coordination Office, Federal News Network (2022).

[12] See Quint Forgey & Daniel Lippman, CIA Launches New China-Focused Unit, Politico (2021). See also Transcript: NPR's Full Conversation with CIA Director William Burns, NPR (2021).

[13] Zach Dorfman & Jenna McLaughlin, The CIA's Communications Suffered a Catastrophic Compromise. It Started in Iran, Yahoo News (2018); Zach Dorfman, Tech Giants Giving China an Edge in Espionage, Foreign Policy (2020).

[14] Samantha Hoffman & Nathan Attrill, Mapping China's Tech Giants: Supply Chains & the Global Data Collection Ecosystem, Australian Strategic Policy Institute (2021).

- *Adapt* to the digital era and geopolitical rivalry by modernizing IC practices to access the best talent, acquire the latest technology, build an integrated community-wide digital infrastructure, and exploit the broadest set of data;

- *Leverage* insights and information from open and commercial sources by creating a dedicated, technology-enabled open source entity to support U.S. decision making;

- *Create* new capacities to capture and master economic, financial, and technological intelligence by establishing a National Techno-Economic Intelligence Center to serve as an economic "nerve center" for U.S. policymakers; and

- *Counter* foreign adversarial influence campaigns through preemptive exposure of their operations, strategic warnings for the U.S. public, alerts for senior U.S. Government officials who may be specifically targeted by such operations, and adoption of new mitigation technologies.

This transition will not be easy, but it is necessary. Policymakers and Congressional leaders must agree to a vision on how to reform the IC based on current technology trends and geopolitical threats. The White House and Congress must then set the direction while IC leaders sustain focus within the bureaucracy for forward movement. The 2022 National Security Strategy took the first step in calling for the IC to adapt organizationally, embrace new digital tools, and better integrate open source materials.[15] The closed nature of U.S. intelligence – an essential requirement for keeping secrets – has often allowed inertia to persist or change to be slow rolled. When united under a common goal, however, the IC is capable of remarkable transformation as it demonstrated most recently after the September 11, 2001 terrorist attacks. The stakes of the moment demand that U.S. intelligence overcome the bureaucratic reluctance or resistance to change. The IC remains essential. Amidst a flood of data and opinion, the IC's emphasis on objectivity and providing insight independent of policy gives it a vital role in supporting leaders grappling with difficult decisions.

Enduring Asymmetries Provide the IC Advantages

The IC benefits from several asymmetries – inherent to the enormous strengths of U.S. society and politics - that give it advantages over its rival intelligence systems. An early evaluation of the Central Intelligence Agency (CIA) illustrates the enduring nature of the IC's strengths. Led by the future Director of Central Intelligence, Allen Dulles, the small survey team observed in 1949 that the United States could become a world-class intelligence power:

> "America has the potential resources, human and material, for the best intelligence service in the world. Within our borders we have every race and nationality, loyal sons speaking every language, traveling and resident in every foreign country. We have a wide geographical base for the development of intelligence work. We have the greatest

[15] National Security Strategy of the United States of America, The White House at 46 (2022).

> reservoir of scientific and technical skills. We have important allies abroad who are ready to join their knowledge to ours."[16]

If anything, the IC's ability to access the best talent and technology the United States has to offer has grown since then. The IC is now more open to talent of any ethnicity and creed than in its past, even if being truly representative of U.S. society is still an ongoing process.[17] More U.S. citizens now accept that the country needs an intelligence capability than when Dulles wrote that passage. In the transition period between World War II and the Cold War, many Americans, including President Harry Truman and senior national security officials, feared the creation of the CIA would lead to an unaccountable secret police.[18] A poll published last year showed that 64 percent of Americans believed intelligence plays a "vital role" in national security and only six percent of Americans believed the United States no longer needs intelligence.[19]

The IC benefits from other asymmetric advantages – including its *ethos of objectivity*, its *national mission*, and its work with *allies and partners*. They provide a critical foundation for why the IC has and can continue to pursue and exploit technology to its fullest potential.

- *The ethos of objectivity and truth ensures the IC focuses on understanding reality.* The IC works to understand the world as it is. Collectors and analysts scan the horizon for consequential developments and inform decision making. They do not try to confirm an overarching theory of history or rightness of an ideology. Instead, U.S. intelligence officers understand their role to "call it like they see it" and to "provide unbiased, objective analysis regardless of policy preferences."[20] This search for truths that adversaries are trying to obscure creates a constant impetus to break through their concealments. Tech-enabled collection is a more certain path to ground truth than relying on a flash of analytic insight or the chance of having the right human source in the right place at the right time.

  The intelligence services of our authoritarian rivals, however, are trapped within the worldview of their country's leadership. Whether it be the whims of a dictator or the Chinese Communist Party (CCP), the Russian and PRC intelligence services face unpredictable, fluctuating limits on what is permissible to say.[21] The costs can be high. Russia's intelligence services, especially the Federal Security Service (FSB), reinforced Russian President Vladimir Putin's prejudices against Ukrainians ahead of the February invasion. For example, the FSB possessed polling data from Ukraine that showed that most Ukrainians would resist invasion; however, the service reportedly continued to feed best-case outcomes to Putin.[22] For the CCP, the centrality of Xi Jinping allows

[16] Allen W. Dulles, et al., A Report to the National Security Council: The Central Intelligence Agency and the National Organization of Intelligence at 17 (1949).
[17] Michael Miner & Lindsay Temes, The Past, Present, and Future of Diversity, Equity, and Inclusion in the American Intelligence Community, Belfer Center for Science and International Affairs (2022).
[18] Harry Howe Ransom, Don't Make the CIA KGB, New York Times (1981); Rhodri Jeffreys-Jones, A Question of Standing: The History of the CIA, Oxford University Press at 23-24 (2022).
[19] Stephen Slick & Joshua Busby, 2020 Public Attitudes on U.S. Intelligence, Chicago Council on Global Affairs (2021).
[20] Beth Sanner, A Former Presidential Briefer Rethinks Truth to Power, Cipher Brief (2022).
[21] Reid Standish, Interview: How Russia's Intelligence Agencies Have Adapted After Six Months Of War, Radio Free Europe (2022); Timothy R. Heath, China's New Governing Party Paradigm: Political Renewal and the Pursuit of National Rejuvenation, Ashgate at 41-56 (2014).
[22] Greg Miller & Catherine Belton, Russia's Spies Misread Ukraine and Misled Kremlin as War Loomed, Washington Post (2022); Philip H.J. Davies & Toby Steward, No War for Old Spies: Putin, the Kremlin and Intelligence, Royal United Services Institute (2022).

his perspective to dominate.[23] Moreover, China's intelligence services pursue nonexistent enemies, because the unquestionable logic of the party's ideology pushes them to find external excuses and scapegoats for the party's failures.[24]

- *The IC serves a national purpose to which it is held accountable.* All IC personnel, like other U.S. Government employees, take an oath "to support and defend the Constitution of the United States against all enemies, foreign and domestic."[25] Consequently, they serve the country rather than any particular political party, leader, or agenda. To fulfill their oath, IC personnel must abide by the laws established by the duly elected representatives of U.S. society, and they must be prepared to defend their activities, budget, and policies in front of Congressional oversight (namely the United States Senate Select Committee on Intelligence (SSCI) and House Permanent Select Committee on Intelligence (HPSCI)) and the Administration. This context provides a sense of analytic independence and mission that pervades the IC. The IC's mission helps unite individuals from all facets of society, allowing the community to benefit from excellence wherever it emerges. This encourages the IC to seek partnerships where U.S. society and private sector can contribute – especially in technology – while giving those partners confidence that their cooperation will serve the national interest.

  By contrast, the PRC and Russian intelligence services serve the CCP and the Kremlin leadership, respectively, rather than their countries or their people.[26] To the extent they exist, accountability mechanisms are about ensuring political loyalty. For example, the CCP committee within the Ministry of State Security (MSS), like all party committees, exists to manage personnel, mete out discipline, and give the party a shadow decision making authority that can override the ministry's normal functioning.[27] Consequently, these intelligence services are plagued by political and familial cliques that shape career prospects, inhibit the spread of new ideas, and incentivize corruption.[28] This separates these intelligence services from their societies. Rather than having real partnerships with society or the tech industry, the MSS, for example, demands and expects results from PRC companies.[29]

[23] Cai Xia, The Weakness of Xi Jinping, Foreign Affairs (2022).
[24] Samantha Hoffman, The Chinese Communist Party Always Needs An Enemy, Foreign Policy (2019); Cai Xia, The Weakness of Xi Jinping: How Hubris and Paranoia Threaten China's Future, Foreign Affairs (2022); Qian Gang, 語象報告：習近平的「敵對勢力」, Storm Media [Taiwan] (2014); Qian Gang, Qian Gangyuxiang Report: "Hostile Forces" and the Age of Stability Maintenance 語象報告：「敵對勢力」與維穩年代, Storm Media [Taiwan] (2014).
[25] 5 U.S.C. § 3331.
[26] The Constitution of the Chinese Communist Party states that new party members must take the following oath of admission: "It is my will to join the Communist Party of China, uphold the Party's program, observe the provisions of the Party Constitution, fulfill the obligations of a Party member, carry out the Party's decisions, strictly observe Party discipline, protect Party secrets, be loyal to the Party, work hard, fight for communism for the rest of my life, always be prepared to sacrifice my all for the Party and the people, and never betray the Party." Admission Oath, China Daily (2010). Nikolai Patrushev, head of Russia's Security Council, described Russian intelligence services as having always been employed as "an instrument of supreme power" in service "of the existing political regime" while serving as Director of the FSB in 2002. See We Serve Russia, Federal Security Service of the Russian Federation (FSB) (2002).
[27] Richard McGregor, The Party: The Secret World of China's Communist Rulers, Harper at 15-17 (2010); Nicholas Borst, Party Committees in Chinese Companies, Seafarer - Prevailing Winds (2021).
[28] Andrei Soldatov & Irina Borogan, The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB, PublicAffairs at 4, 10-11 (2010); Boris Volodarsky, Russian Intelligence Isn't All It's Cracked Up To Be, The Spectator (2022); Alex Joske, Spies and Lies: How China's Greatest Covert Operations Fooled the World, Hardie Grant at 39, 54 (2022).
[29] Zach Dorfman, Tech Giants Are Giving China a Vital Edge in Espionage, Foreign Policy (2020).

- *The IC benefits from a worldwide network of allied and partner intelligence services.* From the creation of the modern U.S. intelligence system in World War II, working with allies and partners has been built into U.S. intelligence.[30] For example, when a covert listening device was discovered in the U.S. Ambassador to Moscow's office in 1952, U.S. officials turned to the U.K.'s Security Service (commonly referred to as MI5) for help in solving the riddle of how "The Thing," as it was later dubbed, worked.[31] Once the inner-workings of the Soviet bug were understood, MI5 engineers succeeded in developing a British variant of it, which was later taken into production and was used in clandestine operations by the British, Americans, Canadians, and Australians in the years following.[32] This collaboration enabled the IC to demystify and deploy a superior variant of "The Thing" to outperform a rival.

  These connections are fundamental to the way the IC operates, and the IC has become adept at finding ways to work securely with nearly any potential partner where mutual benefit could be found. The most notable is the "Five Eyes" collaboration among the United States, United Kingdom, Australia, Canada, and New Zealand across all collection and analytic disciplines. Intelligence cooperation also is embedded within other multilateral and bilateral U.S. alliances, such as the North Atlantic Treaty Organization (NATO) and the U.S.-Japan alliance.[33] Shared intelligence helps create shared understanding, which feeds a sense of common purpose and joint problem solving. These shared perceptions also bolster the objectivity of the IC by injecting outside perspectives, often based on similar information but varied experiences. These relationships, in the words of the White House, are "our most important strategic asset" for U.S. national power.[34]

  U.S. rivals do not benefit, certainly not to this extent, from these kinds of collaborative and free flowing partnerships. Where such relationships are publicly knowable, authoritarian rivals tend toward transactional relationships or ones in which they can dominate.[35] While these states may share an interest in damaging the U.S. and blinding the IC worldwide,[36] these relationships fulfill the needs of the moment. They are built on "micro-agendas" and are not signs of enduring trust or a shared sense of purpose.[37] Forums like the Shanghai Cooperation Organization (SCO), within which China wields the greatest influence, and the Collective Security Treaty Organization (CSTO),

[30] 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).
[31] Peter Wright, Spycatcher, Viking Penguin at 20 (1987); Drawing and Photographs, Russian Resonant Cavity Microphone, FBI Laboratory (1952); Robert Wallace & H. Keith Melton, Spycraft: The Secret History of the CIA's Spytechs, from Communism to Al-Qaeda, Plume at 65-66 (2008).
[32] Robert Wallace & H. Keith Melton, Spycraft: The Secret History of the CIA's Spytechs, from Communism to Al-Qaeda, Plume at 65 (2008); Satyr, Crypto Museum (last accessed 2022); Security Survey of the White House Internal FBI Memorandum (1953).
[33] Michael E. DeVine, United States Foreign Intelligence Relationships: Background, Policy and Legal Authorities, Risks, Benefits, Congressional Research Service (2019).
[34] National Security Strategy of the United States, The White House at 11 (2022).
[35] Walter Süß & Douglas Selvage, KGB/Stasi Cooperation, Woodrow Wilson International Center for Scholars (last accessed 2022).
[36] Zach Dorfman & Jenna McLaughlin, The CIA's Communications Suffered a Catastrophic Compromise. It Started in Iran, Yahoo News (2018).
[37] Russia, for instance, frequently uses institutions it dominates—such as the Collective Security Treaty Organization and the Eurasian Economic Union—to counter the PRC's influence in Central Asia through vehicles like the SCO, despite its formal observer status in said institutions. See Paul Stronski & Richard Sokolsky, Multipolarity in Practice: Understanding Russia's Engagement With Regional Institutions, Carnegie Endowment for International Peace (2020). See also Matthew Crosston, The Strange Case of the Shanghai Cooperation Organization, New Eastern Outlook (2014); Thomas Wallace, China and the Regional Counter-Terrorism Structure: An Organizational Analysis, Asian Security (2014); J. H. Saat, The Collective Security Treaty Organization, Defense Academy of the United Kingdom at 8 (2005).

a Moscow-led military bloc of former Soviet republics, are "chronically underfunded"[38] and lack independent decision making authority.[39] In the case of "The Thing," the United States and its allies were able to use their version of the eavesdropping device against the Warsaw Pact, because the Soviets did not see fit to share the technology with the states they dominated. This lack of trust and partnership created a vulnerability that the IC was able to exploit.

Averting Intelligence Failure in U.S. – PRC Rivalry

The U.S.-PRC techno-economic rivalry emerged quietly. There was no vivid catalyst, such as the burning hulk of the USS Arizona on December 7, 1941, following the attack by Japanese airplanes; the eerie, disembodied electronic chirping of Sputnik as it crossed the night sky in 1957; or the collapse of the World Trade Center towers on September 11, 2001 after the terrorist attacks. Those moments viscerally brought home the need for community-wide transformation. Other moments of international competition like much of the Cold War occurred more gradually. In the same way, a similar moment for today's PRC competition has not and may not happen, despite such technological surprises as the PRC's progress in fifth-generation wireless technologies (5G).[40]

Mindful of this dynamic, building the momentum for sustained IC transformation today requires U.S. leadership not only to fully appreciate the rivalry with the PRC, but also to imagine what an intelligence failure would look like in a state of persistent conflict. Only by fully grasping that the competition and conflict will play out in a series of quiet, accumulating moves will U.S. policymakers and IC leaders be able to identify how to change the community to avert failures and take positive actions to win the competition.

The IC's challenge will not stem from a lack of strategic clarity. The United States – both as a government and a society – increasingly recognizes an existing state of rivalry with the PRC.[41] This recognition crosses party lines and has grown steadily since 2018.[42] A growing body of government and non-government analyses examine the strategic intentions of the CCP domestically and internationally.[43] U.S. policymakers and analysts also know the technology bets Beijing has placed to overcome its internal challenges and achieve advantages over the United States and its allies.[44] There is little doubt about Beijing's intentions

[38] Vladimir Rozanskij, The 30th Anniversary of CSTO, The 'Paper Tiger', Asia News (2022).
While Xi Jinping announced in a 2017 speech that the PRC will contribute an additional 10 million yuan (1.47 million U.S. dollars) to the SCO Secretariat to facilitate its work, it's unclear to what extent that has occured. Richard Weitz, The Shanghai Cooperation Organization (SCO): Rebirth and Regeneration?, International Relations and Security Network (2014); Spotlight: Chinese President's Speech at SCO Summit Praised by Overseas Experts, Scholars, Xinhua (2017).
[39] Vladimir Rozanskij, The 30th Anniversary of CSTO, The 'Paper Tiger', Asia News (2022); Dmitry Gorenburg, Russia and Collective Security: Why CSTO Is No Match for Warsaw Pact, Russia Matters (2020).
[40] Mid-Decade Challenges to National Competitiveness, Special Competitive Studies Project at 18-20 (2022).
[41] National Security Strategy of the United States of America, The White House (2017); Interim National Security Strategic Guidance, The White House (2021).
[42] Laura Silver, et al., Most Americans Support Tough Stance Toward China on Human Rights, Economic Issues, Pew Research Center (2021).
[43] For example, United States Strategic Approach to the People's Republic of China, The White House (2020); 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); Rush Doshi, The Long Game: China's Grand Strategy to Displace the American Order, Oxford University Press (2021); Hal Brands, What Does China Really Want? To Dominate the World, Bloomberg (2020); Liza Tobin, Xi's Vision for Transforming Global Governance: A Strategic Challenges for Washington and Its Allies, Texas National Security Review (2018).
[44] See generally Mid-Decade Challenges to National Competitiveness, Special Competitive Studies Project (2022); Final Report, National Security Commission on Artificial Intelligence at 160 (2021); Outline of the People's Republic of China 14th Five-Year

and the contours of its strategy to achieve what the party calls the "Great Rejuvenation of the Chinese Nation."[45]

Even a potential U.S. intelligence failure on PRC military action against Taiwan – the area most likely to precipitate a U.S.-PRC war – would be a failure of tactical warning rather than a strategic surprise. Beijing has been transparent about its intentions to annex Taiwan, leaving vague only the timeline for allowing peaceful if still coercive means to achieve unification.[46] The IC almost certainly will see any significant CCP military mobilization, like the Russian mobilization ahead of its invasion of Ukraine.[47] A large and significant analytic community, both inside and outside the government, track and analyze the People's Liberation Army. The PRC's potential workarounds for resolving its problems with sealift and amphibious assault, such as hardened roll-on, roll-off ferries, also have been identified.[48] Economic indicators of preparation, including reducing dependency on the U.S. dollar and stockpiling critical supplies, also are known.[49] And dozens of wargames have been used to socialize the challenges of U.S. intervention to defend Taiwan among U.S. decision makers and advisors.[50] In short, the United States, collectively, understands the many ways in which the PRC might launch a war for Taiwan.

Intelligence failures, therefore, probably will not be in the form of not anticipating a war on Taiwan or some other significant policy action, but rather misunderstanding Beijing's logic and purpose behind them. These kinds of failures could undermine the IC's credibility and usefulness. However, they are the kinds of normal failures that naturally occur in intelligence and can be explained by the difficulty of understanding an adversary, cognitive biases, collection shortfalls, and the other problems that routinely appear in such failures.[51] Such intelligence failures rarely, if ever, drive significant organizational changes in the way that the attack on Pearl Harbor and the September 11, 2001 terrorist attacks did.

The greatest risk of failure for the IC is being unable to support the formulation and execution of U.S. strategy to overcome the economic and technological challenges from the PRC. In our report on Mid-Decade Challenges to National Competitiveness, we identified several characteristics of how the world

---

Plan for National Economic and Social Development and Long-Range Objectives for 2035, Center for Security and Emerging Technology (2021); Outline of the 14th FYP; Notice of the State Council on the Publication of "Made in China 2025", Center for Security and Emerging Technology (2022).

[45] Strong Military: Episode I "The Dream",China Central Television (2017); Xi Jinping, Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era, Report to the 19th National Congress of the Communist Party of China (2017).

[46] Anti-Secession Law (Adopted at the Third Session of the Tenth National People's Congress) (2005); Xi Jinping: 40th Anniversary of Issuing "Message to Compatriots in Taiwan", (2019).

[47] John Culver, How We Would Know When China Is Preparing to Invade Taiwan, Carnegie Endowment for International Peace (2022); Shane Harris & Paul Sonne, Russia Planning Massive Military Offensive Against Ukraine Involving 175,000 Troops, U.S. Intelligence Warns, Washington Post (2021).

[48] Conor M. Kennedy, China Maritime Report No. 4: Civil Transport in PLA Power Projection, U.S. Naval War College Chinese Maritime Studies Institute (2019); J. Michael Dahm, China Maritime Report No. 16: Chinese Ferry Tales: The PLA's Use of Civilian Shipping in Support of Over-the-Shore Logistics, U.S. Naval War College Chinese Maritime Studies Institute (2021); Kevin McCauley, China Maritime Report No. 22: Logistics Support for a Cross-Strait Invasion: The View from Beijing, U.S. Naval War College Chinese Maritime Studies Institute (2022).

[49] Gerard DiPippo, Economic Indicators of Chinese Military Action against Taiwan, Center for Strategic and International Studies (2022).

[50] Todd South, In Think Tank's Taiwan War Game, US Beats China at High Cost, Military Times (2022); Stacie Pettyjohn, et al., Dangerous Straits: Wargaming a Future Conflict over Taiwan, Center for a New American Security (2022); Jeremy Sepinsky & Sebastian J. Bae, War-Gaming Taiwan: When Losing to China Is Winning: What Military Planners Learn When They Simulate a Chinese Attack, Foreign Policy (2022).

[51] Jack Davis, Why Bad Things Happen to Good Analysts, in Analyzing Intelligence: National Security Practitioners' Perspectives at 121-135 (2014).

would look if the United States, alongside democratic allies and partners, began losing the techno-economic competition. That world was one in which many, if not all, of the following features became true:

- The PRC's dominance of the next wave of technology generates trillions in economic output and a dominant position in the economy of the future;
- The PRC's tech sphere of influence spans the globe. The PRC uses its techno-economic advantage for political leverage. U.S. allies hedge and states reliant on PRC tech swing into the its political orbit;
- Authoritarian regimes sell the case that they are masters of the modern world and democracies are in decline;
- An open Internet is compromised, replaced by frictionless digital oppression;
- States' digital infrastructure is cyber-compromised;
- The U.S. military's technological edge erodes. U.S. defense commitments and power projection are threatened; and
- The PRC annexes Taiwan and cuts off supply of microelectronics and other critical technology inputs.[52]

The IC has a key role to play in tracking Beijing's intentions and activities in the techno-economic competition, understanding its motivations, and alerting U.S. policymakers to the implications of these moves. As the rivalry plays out on a global scale and with persistent conflict below the level of armed clashes,[53] U.S. policymakers will be consumed by an increasingly diverse set of issues, including technology, on which the IC's exquisite collection may not be cost effective for delivering U.S. advantage. What the United States once treated as matters of business, such as Huawei and ZTE's 5G deployments, are now rightly understood as features of economic conflict. The growth of PRC firms in strategic industries often has been at least as political as it is economic.[54] In 5G, Huawei and ZTE benefited from industrial strategies to undercut foreign competitors, state subsidies and financing,[55] corruption and coercion,[56] and technology theft.[57] Their successes are, in part, a result of the U.S. and others' failures to anticipate and counter the PRC's predatory economic practices.

[52] Mid-Decade Challenges to National Competitiveness, Special Competitive Studies Project (2022).
[53] Repeated acts of aggression by authoritarian governments in China (and Russia), often enabled by advanced and emerging technologies, blur the lines between war and peace. These actions include frequent cyber-attacks, unrelenting disinformation operations, aggressive theft of intellectual property, and sabotage. Even if most of these actions are invisible to many Americans, they leave little doubt that the United States is now in a state of persistent conflict with Russia and China. See Mid-Decade Challenges to National Competitiveness, Special Competitive Studies Project at 124 (2022).
[54] David Feith & Rick Switzer, China Hit Some Bumps on Its Road to Semiconductor Dominance, Wall Street Journal (2022); Xiao Cen, et al., A Race to Lead: How Chinese Government Interventions Shape U.S.-China Production Competition, SSRN Working Paper (2022).
[55] Chuin-Wei Yap, State Support Helped Fuel Huawei's Global Rise, Wall Street Journal (2019).
[56] Testimony of Andy Keiser before the U.S. House Committee on Small Business, ZTE: A Threat to America's Small Businesses (2018); A Transactional Risk Profile of Huawei, RWR Advisory Group (2018).
[57] Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets, U.S. Department of Justice (2020); Chinese Telecommunications Device Manufacturer and its U.S. Affiliate

The second measure of the IC will be its ability to enable U.S. policy implementation in the rivalry with the PRC by identifying points of leverage and impact in real time. The U.S. Government, including some of its most seasoned diplomats, has struggled with identifying the leverage it possesses over the PRC and how to apply it effectively.[58] This requires the IC to have persistent visibility into the CCP's political situation so that U.S. leaders can better time and target their actions to influence Beijing's decision-making. The IC also needs to be able to help target U.S. policy actions for maximum impact, particularly in technological and economic areas. These are all issues where publicly and commercially available information probably provides more cost-effective data and insights than the IC's unique capabilities.[59] From the collection or acquisition of this information through its analysis and dissemination, AI-enabled tools and the related technology architecture can make each process more efficient, faster, and comprehensive.

Adapting U.S. Intelligence for the Digital Era

How should the Intelligence Community reorient itself to harness the opportunities offered by AI and the digital era?

The rivalry with the PRC challenges the U.S. Government across the board – not just the traditional national security agencies. More officials will be more directly engaged in competitive actions to wield all the elements of national power, especially as they relate to economic, scientific, and technological issues. To serve the broadening and diversifying intelligence needs of the techno-economic rivalry, the IC needs to expand its use of AI and other emerging technologies. These tools will enable the IC to better turn its troves of data into a wealth of intelligence that enables U.S. policymakers to act more effectively. Mastering the tools of the digital age will require a transformation that must be pushed from the top and involve finding new ways to resolve the challenges of incorporating the right talent and technologies.

U.S. Government leaders inside and outside the IC will need to devote their attention to digital transformation if AI and emerging technologies are to fulfill their potential to transform the IC. Top-down leadership is needed to drive and sustain this transformation. Success in AI and emerging technologies starts with the right leadership culture that is committed to the endeavor and willing to devote time and resources.[60] Transformation requires adherence to a coherent vision that aligns strategies, actions, incentives, and metrics. IC leaders must understand AI and emerging technologies – their benefits and limitations – to maximize the opportunities the technology can offer.

Creating a technology- and AI-enabled IC will also need to be a community-wide effort. Over the years, the IC has developed several AI strategies and implementation plans,[61] but they have been unevenly

Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction Of Justice, U.S. Department of Justice (2019); Phil Wahba & Melanie Lee, Motorola Sues Huawei for Trade Secret Theft, Reuters (2010).

[58] Susan Thornton, This Is How Biden Can Get the Edge Over China, New York Times (2021); Richard Nephew, China and Economic Sanctions: Where Does Washington Have Leverage?, Brookings (2019).

[59] For example, the CCP's structure and the need to mobilize its millions of cadres spread across the country at multiple levels of governance often requires it to communicate in the open. See Rush Doshi, The Long Game: China's Grand Strategy to Displace American Order, Oxford University Press at 32-37 (2021).

[60] Tomas Chamorro-Premuzic, et al., As AI Makes More Decisions, the Nature of Leadership Will Change, Harvard Business Review (2018).

[61] See, e.g., The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines, Office of the Director of National Intelligence (2019); NGA Releases New Data Strategy to Navigate Digital, GEOINT Revolution, National Geospatial-Intelligence Agency (2021).

implemented across the community and individual agencies. The IC needs a single, cohesive strategy for transformation to turn isolated initiatives into a community-wide technological revolution. IC leaders and their designated technology leadership should prioritize projects that build internal tech expertise, improve data standardization and architecture, and support emerging tech adoption at scale across the IC.

AI Utility for Intelligence

Tasking

- Sequencing and deconflicting the tasking of intelligence platforms efficiently across collection disciplines.
- Detecting and prioritizing targets of interest by analyzing patterns that suggest opportunities to collect unique information or exploit vulnerabilities.
- Assisting decision-makers in identifying information requirements and prioritizing collection targets.

Collection

- Identifying potential opportunities for collection by finding gaps in tech-enabled counterintelligence and security systems as well as alternative collection pathways to an intelligence target.
- Automating the validation process by cross-checking collection across all other reporting and collection disciplines.
- Enabling smart sensors at the edge to improve collection fidelity and trigger collection when necessary.

Processing

- Transforming unstructured data into a structured queryable, filterable, sortable, and digestible data to aid analysis.
- Employing natural language processing to transcribe, translate, and summarize foreign language materials.
- Summarizing raw intelligence reporting with critical information highlighted and tailored for analysts.

Analysis

- Accelerating pattern matching and anomaly detection across intelligence disciplines and the intelligence record.
- Generating visualizations to illustrate relationships, networks, geographies, and time lapses.
- Automating portfolio-specific indications and warning alerts for analysts.

Dissemination

- Tracking usage and impact of disseminated intelligence reporting and analysis.
- Automating the creation and delivery of finished and raw intelligence to the appropriate users and analysts at any level of classification.
- Streamlining classification downgrading to facilitate intelligence sharing with other U.S. Government agencies, allies, and private industry.

Business Practices

- Systematizing the auditing and approval process for routine business practices, such as accounting, as well as flagging anomalies for manual review.
- Monitoring IT systems to provide predictive maintenance and upkeep requests.
- Supporting the workflow and review requirements for Contracting Officer's Technical Representatives through a project's life cycle.

Security

- Enhancing physical security measures by enhancing network video surveillance, trace detection, and other intrusion detection systems.
- Augmenting security clearance investigation and continuous evaluation.
- Mapping supply chains of Intelligence Community vendors and equipment.

The Director for National Intelligence (DNI), Undersecretary of Defense for Intelligence, and the directors of the CIA, Defense Intelligence Agency (DIA), National Geospatial Agency, National Reconnaissance Office, and National Security Agency, in particular, must take the lead because their agencies are well-equipped to serve national missions. They also are uniquely positioned to lead their own staff and agency in transforming the bureaucracy. To the extent that they delegate the implementation to chief technology officers, chief data officers, and governance bodies, those technology leaders will only be effective if given the staff, money, and convening and decision power to determine how their agencies move forward.

Another avenue to foster transformation is by ensuring that future promotions into the senior executive service ranks will require experience, when possible, or executive education on AI and emerging technologies.[62] Management roles at lower levels should similarly require education and training when handling the development and application of technology in operational settings. Without a structured learning process for updating leadership on the current technological state of the art, IC leadership could be trapped in past generations of technology in which they were expert or have experience. Elements of executive technology education could be incorporated into the war college experience, executive courses at U.S. universities, and ongoing speaker series or modules. Because the user experience is critical to how technology and software applications are actually applied, a practical element done in a live IC setting should be considered as part of any education or training program. AI-enabled tools have the ability to fundamentally transform the work at lower levels in the IC. As a result, senior leaders not recently in those positions or with current practical exposure to AI-enabled tools may have propositional rather than practical understandings of their subordinates' work. To ensure level-setting of practical understanding, executive education and training should occur when a manager is in between positions rather than on top of existing job responsibilities. Although the immediate need is executive education, the pace of technological change requires a culture of learning throughout a career.

Successful, at-scale digital transformation requires the right combination of people, processes, and technology. The IC requires a broad foundation to ensure that emerging technology services can be built, scaled, and effectively employed across mission areas. It needs *people* with the right expertise to advance technology; *processes* to enable the convergence and teaming of humans and technologies; and the right *technology* to store, process, and move data at immense scale across the community. Integrating these elements is a challenge for any large enterprise, upsetting traditional career paths, workflows, data management, and technology integration. Shifting the IC's practices will require standardizing and contextualizing data for broader use, building a new digital backbone, and accessing necessary talent. As these elements come together, the IC would gain agility and efficiency in honing existing applications and applying them to new problems.

To integrate the people, processes, and technology effectively, the IC should prioritize flexible teams and diverse expertise. Outdated or somewhat rigid human resource policies and career services undermine how teams can form as well as the individual's growth and development as a professional. Digital transformation requires expertise in fields like data science, software development, business analytics, and enterprise software management. These fields evolve quickly and require professionals to have the option for external engagements that keep their knowledge current. Moreover, the IC's requirements for these skill sets will change over time. Ultimately, this problem of balance might be best addressed under

[62] Tomas Chamorro-Premuzic, et al., As AI Makes More Decisions, the Nature of Leadership Will Change, Harvard Business Review (2018); Andrew Ng, AI Transformation Playbook, Landing AI (2020).

a broader, more flexible digital career service than trying to coordinate across several, narrower career services.

Recommendation: *Create a Digital Experimentation and Transformation Unit*

The DNI should sponsor the creation of a Digital Experimentation and Transformation Unit to run pilot projects that address community-wide challenges on talent, processes, technologies, or acquisition as identified by the DNI and IC agency directors. The unit should be sponsored and empowered by the DNI, with one of the intelligence agencies serving as the executive agent, and with representatives from each member of the IC. The purpose would be to identify and apply the best available technology and expertise in the United States, inside and outside government, to select community-wide problems. The DNI would also need support from Congressional appropriators to ensure the office has the necessary time and support to solve the selected problems. The pilot projects should address a key aspect of the people, processes, technology, and acquisition needs of the IC to accelerate its digital transformation. All projects would need to include programmatic analysis for each participating IC element to ensure successful projects are sustained beyond the new unit. The initial focus areas could include:

- The recruitment, vetting, and employment of personnel that possess needed expertise and/or meet some high-risk criteria;
- The improvement of IT systems interoperability across the IC;
- The automation of cross-collection platforms tipping and queuing at the edge to improve IC indications and warning capabilities; or
- The creation and management of an IC-wide knowledge management platform that serves as a repository for algorithms, training data, and internal IC ideas network.

To effectively counter adversaries and maximize the Intelligence Community's potential, U.S. intelligence and its external government stakeholders must also redefine their sense of risk. Avoiding risks in the short term is a sure way of creating long-term risks for intelligence failures. As the speed of information, technological innovation, and decision-making accelerate, the IC should reevaluate the risk across all aspects of the enterprise – including how data is shared, how technology is acquired, and how talent is recruited. This reevaluation must also include the risk of incremental changes or doing nothing. Sometimes, doing nothing can be the riskiest choice of all. Internally, this includes providing space for experimentation, tolerating failures, and ensuring that security practices support the intelligence mission. Externally, the IC must partner with Congress and the White House so that external stakeholders accept reasonable risk taking.

Building the conditions for a tech-enabled Intelligence Community also requires new security approaches that bring critical expertise and technology into the community. The IC has an opportunity to update its security practices and redefine the meaning of successful security. Success should be the safe employment of people, including those with direct, in-country experience in rival countries, or with expertise in

technology needed to execute its digital age mission facing an all-domain rival. These security practices also slow down the adoption of needed, advanced commercial technology in favor of retaining older, government-approved technology.[63] The IC needs dynamic, digital age-aware security practices that are fully aligned with overall national security and IC objectives.

U.S. intelligence leadership and external stakeholders need to revisit security processes and the preoccupation with counterintelligence risk minimization. Risks cannot be avoided in the world in which the IC is operating. Attempting to do so places barriers between U.S. intelligence and the resources, both human and technological, needed to adapt to the rivalry with the PRC and the digital era. The current security system was originally constructed to address threats against IC interests that exploited relatively small, stable, and predictable attack surfaces - namely, its people. The individualization of data, mobile telecommunication, social media, and the centralization of personnel information on databases creates opportunities for hostile intelligence services to target IC employees and contractors without ever coming face to face with the individual.[64] The attack surfaces that security now seeks to protect are constantly expanding and evolving in unpredictable ways.[65] Yet, the fundamentals of how people and technology are cleared have not significantly changed in decades.[66]

The inability to clear qualified applicants who have spent significant time in the PRC suggests the clearance process has fundamental problems.[67] The experience inside the country may give PRC intelligence services the first opportunity to recruit them, and the PRC's intent to recruit potential applicants to the IC is well documented.[68] However, not every U.S. citizen is vulnerable to recruitment by a foreign intelligence service, nor are those vulnerable necessarily recruited. An inability to identify these individuals means that the security officials deciding on clearances have inadequate heuristics for determining current and predicting future loyalty. Without better ways to measure risk and identify loyal Americans, the logic of minimizing risk and making faster decisions will always push investigators toward not clearing individuals with higher risk profiles, like those who have lived or studied in the PRC. Improvements to the process would lower the risks of speeding up the clearance process and ensure the IC brings in the necessary expertise and talent for digital era rivalry with the PRC.

Accessing tech-savvy talent requires the Intelligence Community to adopt more flexible approaches for hiring and retention. The IC possesses three advantages over the private sector that ensure people will want to join, and even return, to public service. The first is a sense of purpose. The second is a unique

[63] Emily Harding, Move Over JARVIS, Meet OSCAR, Center for Strategic and International Studies at 2 (2022).
[64] Digitalization of data and the spread of computers expanded the potential attack vectors again and the ability to identify who and where someone was. See Warren Strobel, Biometrics, Smartphones, Surveillance Cameras Pose New Obstacles for U.S. Spies, Wall Street Journal (2021); Hardware vulnerabilities were joined by software vulnerabilities. More and more equipment and software used by the government were commercial off-the-shelf (COTS) products – all of which could be exploited directly or through supporting services and the supply chain. See e.g., ASUS Software Updates Used for Supply Chain Attacks, Symantec Security (2019); Dina Temple-Raston, A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack, National Public Radio (2021).
[65] Corin Stone, Artificial Intelligence in the Intelligence Community: Money is Not Enough, Just Security (2021); Robert Wallace & H. Keith Melton, Spycraft: The Secret History of the CIA's Spytechs, from Communism to Al-Qaeda, Plume at 223 (2008).
[66] David Luckey, et al., Assessing Continuous Evaluation Approaches for Insider Threats: How Can the Security Posture of the U.S. Departments and Agencies Be Improved?, RAND Corporation (2019).
[67] Promoting Cultural Diversity in the Intelligence Community: Recruiting and Clearing Personnel with Foreign Ties, Intelligence and National Security Alliance (2022); The China Deep Dive: A Report on the Intelligence Community's Capabilities and Competencies with Respect to the People's Republic of China, House Permanent Select Committee on Intelligence at 28 (2020); Kenneth Lieberthal, The U.S. Intelligence Community and Foreign Policy: Getting Analysis Right, Brookings at 32-33 (2009).
[68] See, e.g., Peter Mattis, Shriver Case Highlights Traditional Chinese Espionage, China Brief (2010); Game of Pawns, U.S. Federal Bureau of Investigation (2013).

problem set. The third is a sense of stability. However, the IC – and the U.S. Government more broadly – will continue to be challenged to compete directly with the private sector for compensation. Salaries for AI talent, in particular, continue to rise along with the demand in the private sector. The competition for technical expertise in the current market puts the IC at a disadvantage in hiring top-level talent.[69] Beyond this technical talent, the IC also needs people adept at shaping how the community manages AI and other emerging technology. In addition to incentivizing software programming skills as described in the next section, the IC should seek to expand talent related to AI architecture,[70] data warehousing, and Software as a Service (SaaS).

More flexible approaches to recruitment and career development would allow the IC to better harness expertise and stay at the cutting edge of technological development. The current personnel system generally does not reward individuals who move between the private sector and the IC. This internal orientation was less of a problem when significant technological innovation occurred inside the government, but the private sector has taken the lead in emerging technologies.[71] Only by allowing or facilitating government employees to move in and out of government or by developing personnel exchange or fellowship programs with the private sector will the IC ensure it has regular access to talent knowledgeable and capable of applying leading technologies. The National Reserve Digital Corps, proposed by the National Security Commission on Artificial Intelligence (NSCAI), could enable those who move to the private sector to continue to support the IC.[72] Yet another talent pipeline for the IC, in this case for full-time talent, could be a potential U.S. Digital Service Academy, also proposed by the NSCAI.[73]

The IC can get talent through the door, but has trouble with placing and developing talent in ways that challenge the community's ability to retain technology talent. Technical specialists have all too often found themselves placed in the wrong position for their skills, while internal personnel policies prevent them from finding a new position. Although some stay and change to a new position when the opportunity arises, others simply leave. As one senior U.S. Government data officer noted, the government can attract experienced and proven AI talent, but should only expect them to stay for three to four years before they move on.[74] Likewise, while IC agencies provide useful training in agency-specific tradecraft and skills, they are not regularly supportive of developmental opportunities for data scientists, software developers, and other digitally-oriented skills. Meanwhile, the pace of development in the private sector moves quickly and, without developmental opportunities outside the community, the IC's talent will lag or leave.

---

[69] Cade Metz, A.I. Researchers Are Making More Than $1 Million, Even at a Nonprofit, New York Times (2018); The Senior Executive Service pay scale by contrast, tops out at $226,300. See Salary Table No. 2022-EX, U.S. Office of Personnel Management (2022).

[70] AI architects play a central role in bringing together the various components needed to build and scale AI initiatives. See Ashutosh Gupta, What Are AI Architects and What Do They Do?, Gartner (2022).

[71] Zachary Arnold, et al., Tracking AI Investment: Initial Findings From the Private Markets, Center for Security and Emerging Technology (2020).

[72] The National Reserve Digital Corps, as envisioned by the NSCAI, would bring in digital expertise as civilian special government employees (SGEs) to work at least 38 days each year in government. The military reserves' service commitments and incentive structure would serve as the program's model. See Final Report, National Security Commission on Artificial Intelligence at 10, 358-362 (2021). In June 2021, U.S. Representatives Tony Gonzales and Robin Kelly introduced legislation to form a National Digital Reserve Corps, which has since been referred to the House Committee on Oversight and Reform. See H.R.4818, National Digital Reserve Corps Act, 117th Congress (2021).

[73] Final Report, National Security Commission on Artificial Intelligence at 127 (2021). For additional detail on technology talent pipelines for the U.S. Government, see Mid-Decade Challenges to National Competitiveness, Special Competitive Studies Project at 55-81 (2022).

[74] SCSP Staff Engagement (September 2022).

As it moves to become AI-enabled, the Intelligence Community can learn from other complex organizations, while adapting the lessons to its specialized missions. Large, complex companies across a range of industries and employing tens of thousands of people have moved from the industrial age to the digital age by integrating AI and other emerging technologies throughout their operations. The IC has a unique mission and may have unique features, but some of the core principles for digital transformation appear consistent and can be adapted and leveraged to the IC's needs. These principles include a commitment from leadership, integrated digital infrastructure, and organizational capacity – all developed and applied in stages over time. But the private sector also provides negative examples of how AI initiatives fail. By treating digital transformation as a series of disconnected, independent experiments, rather than a disciplined, multi-stage process, organizations set themselves up for failure.[75] Beginning with a focused leadership aligned behind a single strategy for digital transformation, U.S. intelligence should progressively move its people, processes, and technologies through a series of phases.[76]

The IC and other U.S. Government organizations often are right to be skeptical of the applicability of business practices to public sector work. As business researcher Jim Collins observed, "many widely practiced business norms turn out to correlate with mediocrity, not greatness."[77] This correlation is important to bear in mind as the IC carries out goals aimed at sustaining excellence throughout the transformation. Nevertheless, the kinds of changes presented by these models are built on principles for allowing workers to make more effective and efficient use of data, regardless of the exact work and organizational purpose.

Leveraging Open Source Capabilities

In an age where most data resides in the open world,[78] the IC risks irrelevance if it does not maximize its use of open sources throughout the intelligence enterprise. The exponential growth in publicly and commercially available information has outpaced the IC's capability, or anyone's for that matter, to harness open source in support of U.S. decision making and policy.[79] This has come on top of the decline in the collection, processing, and usage of open source materials through the evolution of IC open source initiatives from the Foreign Broadcast Information Service (FBIS) to the Open Source Center to the Open Source Enterprise (OSE). Moreover, less attention to collection, user-unfriendly platforms, and overzealous security practices limited U.S. intelligence analysts' effective access to and use of government open source resources over time.[80]

[75] Andrew Ng, AI Transformation Playbook, Landing AI (2020).
[76] For an example of one such maturity model, see Marco Iansiti & Satya Nadella, Democratizing Transformation, Harvard Business Review (2022). The research into corporate digital transformation underpinning the model comes from more than 100 companies, illustrating a general path to success. See also Tomas Chamorro-Premuzic, et al., As AI Makes More Decisions, the Nature of Leadership Will Change, Harvard Business Review (2018); Andrew Ng, AI Transformation Playbook, Landing AI (2020); Manasi Vartak, How to Scale AI in Your Organization, Harvard Business Review (2022).
[77] Jim Collins, Good to Great and the Social Sectors: Why Business Thinking is Not the Answer, Harper Business at 1 (2005).
[78] The International Data Corporation estimated that the amount of data in the world would increase from 33 Zettabytes (ZB) in 2018 to 175 ZB by 2025. One ZB is one trillion gigabytes. See David Reinsel, et al., The Digitization of the World from Edge to Core, International Data Corporation at 7 (2018).
[79] Report to the President of the United States, The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction at 23, 377-380 (2005); Heather J. Williams & Ilana Blum, Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise, RAND Corporation (2018); Cortney Weinbaum, et al., Options for Strengthening All-Source Intelligence: Substantive Change Is Within Reach, RAND Corporation (2022).
[80] SCSP staff engagement with open source experts (June 2022).

The value of open source is difficult to overstate, owing to its volume and availability. Open source intelligence, which is "produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement,"[81] also has the power to replace or complement some accesses that were once gained only through more dangerous and costly traditional intelligence-collection platforms.

Within the techno-economic competition, the first signs of policy shifts by adversaries are most likely to come through publicly and commercially available information. Open source research has also validated U.S. claims about the malign activities of the PRC and Russia, which further enabled public discourse unbounded by security concerns about sources and methods. Private researchers exposed the CCP's efforts to spread surveillance technology, acquire foreign technology on a vast scale,[82] the party's political influence operations,[83] gray zone activities in the South China Sea,[84] further development of nuclear weapons,[85] and human rights abuses.[86] The private research firm Bellingcat exposed Russia's hand in the downing of Malaysia Airlines Flight 17, war crimes in Syria, as well as the assassination and surveillance teams behind the attempts on the lives of Russian dissidents and defectors in Europe.[87] These applications represent a fraction of the possible insights generated from publicly and commercially available information in combination with AI-enabled analytic tools.

The integration of open source data as part of an automated intelligence cycle could enable and focus clandestine intelligence collection on the most important collection targets. AI models can also be employed to help label, classify, cluster, and connect open source data to publicly validate U.S. claims about the malign activities of the PRC and Russia without compromising the IC's sources and methods. Despite the promise of open source, momentum for and interest in wider and deeper integration varies widely.[88] IC agencies appear to be following their own approach to meet their own needs.[89]

Calls for an effective open source entity date back to the Cold War.[90] IC experts have long estimated that over 80 percent of the information needed to support intelligence, military operations, public diplomacy, and other policy initiatives can be acquired publicly or commercially.[91] As the potential of publicly available information grew well beyond print and broadcast media, so too did the calls for improvements

[81] Public Law 109-163, National Defense Authorization Act for Fiscal Year 2006, § 931(a)(1) (2005).
[82] William C. Hannas, et al., Chinese Industrial Espionage: Technology Acquisition and Military Modernization, Routledge (2013); Alex Joske, Picking Flowers, Making Honey: The Chinese Military's Collaboration with Foreign Universities, Australian Strategic Policy Institute (2018).
[83] John Fitzgerald, Taking the Low Road: China's Influence in Australian States and Territories, Australian Strategic Policy Institute (2022); China's Influence and America's Interests: Promoting Constructive Vigilance, Hoover Institution (2019); Anne-Marie Brady, Magic Weapons: China's Political Influence Activities Under Xi Jinping, Wilson Center (2017); Clive Hamilton & Mareike Ohlberg, Hidden Hand: Exposing How the Chinese Communist Party is Reshaping the World, Oneworld (2020).
[84] Bonny Lin, et al., A New Framework for Understanding and Countering China's Gray Zone Tactics, RAND Corporation (2022).
[85] Brad Lendon, China is Building a Sprawling Network of Missile Silos, Satellite Imagery Appears to Show, CNN (2021); Matthew Loh, China Building 300 Missile Silos That Could Grow Nuclear Capacity Beyond Russia's or America's: Report, Insider (2021).
[86] Adrian Zenz, Beyond the Camps: Beijing's Long-Term Scheme of Coercive Labor, Poverty Alleviation and Social Control in Xinjiang, Journal of Political Risk (2019); Annual Report 2021, Congressional-Executive Commission on China at 43-227 (2022).
[87] Joshua Yaffa, How Bellingcat Unmasked Putin's Assassins, The New Yorker (2021).
[88] Justin Doubleday, Spy Agencies Look to Standardize Use of Open Source Intelligence, Federal News Network (2022).
[89] Id.; Justin Doubleday, State Department Intelligence Arm to Set Up Open Source Coordination Office, Federal News Network (2022); Byron Tau & Dustin Volz, Defense Intelligence Agency Expected to Lead Military's Use of 'Open Source' Data, Wall Street Journal (2021).
[90] Herman L. Croom, The Exploitation of Foreign Open Sources, Studies in Intelligence (1969).
[91] Richard A. Best Jr. & Alfred Cumming, Open Source Intelligence (OSINT) Issues for Congress, Congressional Research Service at 4 (2007); Anthony Olcott, Open Source Intelligence in a Networked World, Bloomsbury at 17 (2014).

to the IC's open source capabilities.[92] In more recent years, independent commissions and various studies have reiterated these calls. The 2005 Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction stated the "Intelligence Community does not have an entity that collects, processes, and makes available to analysts the mass of open source information that is available in the world today."[93] Subsequent studies of open source intelligence have reinforced the need for a central entity within the IC or U.S. Government.[94] Such an entity should strive to do even more than "enhanc[e] integration of open source material," as the recently-released National Security Strategy suggests, and enable broader acquisition and collection of such materials.[95] While calls for an open source organization are not new, the United States can no longer ignore the value of publicly and commercially available information; the urgency of the techno-economic competition demands action immediately.

A necessary first step in harnessing the potential of open source data is for all U.S. Government departments and agencies to significantly improve their sharing of information with one another, which is encouraged by the current Federal Data Strategy.[96] But the other critically important step is for the IC and, even more broadly, the U.S. Government to address the collection, acquisition, and processing of *foreign* publicly and commercially available information. To meet this demand, the U.S. Government should adopt a two-part approach that (1) internally advances open source reforms and (2) establishes a new institutional home for open source. These two paths are designed with interlocking and mutually reinforcing actions that should be taken together.

All IC elements should undertake a series of internal steps to (1) demonstrate the importance of open source; (2) to build the talent needed to work on open sources; and (3) to equip personnel with the tools that are essential for open source work.

1. *Encourage Open Source Experimentation with "Tiger Teams"*

   The DNI should charge individual IC entities with assembling "Tiger Teams"[97] to experiment with open sources on issues of strategic interest. A Tiger Team could, for instance, be formed to assess publicly and commercially available data for comparison with classified products. Another team could be brought together to try and solve vexing intelligence issues by exploiting open source intelligence only. In both scenarios, Tiger Teams would be encouraged to leverage AI tools, and thus simultaneously demonstrate the utility of both AI and open source data to intelligence analysis writ-large.

2. *Build Workforce Expertise through the Integration of Modernized Incentive Structures*

[92] Preparing for the 21st Century: An Appraisal of U.S. Intelligence, Commission on the Roles and Capabilities of the United States Intelligence Community at xxi, 88-89 (1996); Roadmap for National Security: Imperative for Change, U.S. Commission on National Security/21st Century at xiv (2001).
[93] Report to the President of the United States, The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction at 23 (2005).
[94] Heather J. Williams & Ilana Blum, Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise, RAND Corporation (2018); Cortney Weinbaum, et al., Options for Strengthening All-Source Intelligence: Substantive Change Is Within Reach, RAND Corporation (2022).
[95] National Security Strategy of the United States of America, The White House at 46 (2022).
[96] Federal Data Strategy, U.S. Office of Management and Budget (last accessed 2022).
[97] A term referring to a diverse group of experts who are tackling a specific problem and that suggests alertness and a readiness to pounce.

Directors of CIA and DIA, the assistant secretary of state for intelligence and research, and other all-source analytic leaders should work with the DNI and Office of Personnel Management (OPM) to establish or expand incentives programs similar to the U.S. Air Force's initiative,[98] to reward analysts with a demonstrated proficiency in computer programming languages like Java, SQL, Javascript, C++, and Python. Just as many human-based languages exist, there are an array of computer programming languages that programmers can use to quickly and efficiently process large and complex swaths of information. Similar to how CIA-run foreign language incentive programs have been pivotal in increasing the number of language-capable officers, this program could increase the number of IC analysts proficient in computer programming languages that could be applied to open source work.

3. Equip Personnel with Essential Tools

IC analysts and collectors should have access to basic tools and training to include publicly available information in their work. At a minimum, they should have convenient, non-attributable access to the Internet, Internet research and tradecraft training, and, at the team level, money to purchase account-specific subscriptions. This would allow analysts to more easily keep up with the kind of information naturally coming to policymakers and ensure they make unique contributions. Convenient access to the Internet has ebbed and flowed over time, depending on the agency, and there is no agreed-upon tradecraft that is followed across the IC. Concerns about security have driven decisions to restrict such access. Apart from flagrant misuse or poor tradecraft such as searching directly for information drawn from raw intelligence, security concerns about exposing IC requirements are likely overblown. Many topics traditionally the sole purview of the IC – including a rival's covert influence operations,[99] the structure of a signals intelligence organization,[100] the ownership network of a rival's military equipment[101] and investments,[102] the location of a rival's tunnel complex to hide and transport its nuclear missiles[103] – are now being researched by independent researchers, think tanks, and private sector companies. The IC no longer possesses a unique signature based on the topic or searches.

The U.S. Government should create a new, well-resourced institutional home for open source collection, acquisition, processing, and analysis. The difficulties and costs of collecting open source data, the specialized skills required to handle such data, and privacy concerns related to some of the data suggest that this mission can only be addressed by an entity tailored for the task. A clear institutional home would provide clarity of purpose and mission focus.

As foreign targets learn how researchers or governments might exploit publicly available information to inform future policy actions, they can be expected to adjust and adapt their activities accordingly –

[98] Joe Pappalardo, The Air Force Will Treat Computer Coding Like a Foreign Language, Popular Mechanics (2018).
[99] Alex Joske, Spies and Lies: How China's Greatest Covert Operations Fooled the World, Hardie Grant (2022); Devin Thorne, 1 KEY FOR 1 LOCK: The Chinese Communist Party's Strategy for Targeted Propaganda, Recorded Future (2022); Jack Stubbs, et al., Likes for Lorestan, Graphika (2021).
[100] Mark Stokes, et al., The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure, Project 2049 (2011).
[101] Gregory B. Poling, et al., Pulling Back the Curtain on China's Maritime Militia, Center for Strategic & International Studies (2021).
[102] Ryan Fedasiuk, et al., Harnessed Lightning: How the Chinese Military is Adopting Artificial Intelligence, Center for Security and Emerging Technology (2021).
[103] Phillip Karber, Strategic Implications of China's Underground Great Wall, Georgetown University (2011); see also Hui Zhang, China's Underground Great Wall: Subterranean Ballistic Missiles, Belfer Center for Science and International Affairs (2012).

changing URLs, putting access controls in place, altering content, or even removing it entirely.[104] The U.S. Government needs to position itself now to exploit such closing windows of opportunity. With U.S. rivals also increasingly aware of what open source researchers are doing online and the potential policy consequences of such research,[105] professional tradecraft is more frequently needed to access quality open source information across barriers put up by rivals, such as requirements for true names, local phone numbers, and official identification numbers.[106]

Furthermore, the cost and privacy concerns associated with commercially available information require deliberate acquisition and management efforts. Private companies now have their own sensors. They collect digital data on a range of relevant economic and human activities. Such data, however, is not free. More importantly, it can include information on U.S. persons, necessitating careful handling to protect their privacy and to ensure that agencies receive only the data they are allowed to receive.

While the precise organizational model for an open source entity is secondary to ensuring that it meets the U.S. Government's needs, there are several options that the U.S. Government can choose from to address the imperative of the open source mission. In assessing the various options, policymakers should consider what attributes an entity would need to effectively lead open source intelligence, including:

- ***Expertise.*** A new entity should develop and sustain expertise, meaning it must have the contextual knowledge required for effective work with publicly available information. An open source office must also encourage expertise building through the creation of career paths for analysts and collectors that emphasize time on target and promotions based on demonstrated expertise.

- ***Voice.*** A new entity should be connected to and have a voice in IC processes and structures (e.g., National Intelligence Council), even if it exists outside the IC, so that it can play a role in pushing broader IC performance. In this vein, it should employ a hybrid workforce with cleared and uncleared personnel. Fully cleared personnel are vital to ensuring the connection between open source and clandestine intelligence activities remains open.

- ***Access.*** To facilitate the widest distribution of the material inside of the U.S. and allied governments, write-to-release products from raw information should be undertaken at the lowest classification level. Finished products should also be made publicly accessible in accordance with the copyright, intellectual property, and U.S. persons privacy protections to which each agency must adhere.[107]

- ***Missions.*** A new entity should have clear collection, processing, and dissemination missions. Current open source challenges are not only analytical in nature. We need to also fix the collection side. The

[104] SCSP Open Source Working Group (February 2022); Stephanie Yang, As China Shuts Out the World, Internet Access from Abroad Gets Harder Too, LA Times (2022); Sébastian Seibt, China's Data 'Disappearance' Makes Information Access Rough Going for Outsiders, France 24 (2021); Glenn D. Tiffert, Peering down the Memory Hole: Censorship, Digitization, and the Fragility of Our Knowledge Base, The American Historical Review (2019).
[105] Sébastian Seibt, China's Data 'Disappearance' Makes Information Access Rough Going for Outsiders, France 24 (2021); Luo Jiajun & Thomas Kellogg, Verdicts from China's Courts Used to Be Accessible Online. Now They're Disappearing., ChinaFile (2022).
[106] Josh Chin, China Is Requiring People to Register Real Names for Some Internet Services, Wall Street Journal (2015).
[107] In this context, "U.S. persons" refer to the definition established in Executive Order 12333 related to authorized United States intelligence activities. Under this definition, a U.S. person is a citizen of the United States; an alien lawfully admitted for permanent residence; an unincorporated association with a substantial number of members who are citizens of the United States or are aliens lawfully admitted for permanent residence; or a corporation that is incorporated in the United States. See Executive Order 12333, United States Intelligence Activities, The White House (as amended 2008).

collection of open sources, especially from strategic rivals like the PRC, is becoming a significant challenge. The need to use local phone and identification numbers, for example, introduces ethical considerations into open source work that should not be left to individual all-source analysts.

- ***Gateway.*** A new entity should act as a coordination and distribution hub for open source information between policy agencies, the IC, and external actors. It should enable IC elements and U.S. Government (USG) agencies to access open source data for their own queries and products while also having the authorities to liaise with allies and partners. The intensity and stakes of the current techno-economic competition require a higher degree of shared knowledge and understanding across U.S. society.

- ***Dissemination.*** Open source products should be considered as a utility available to all U.S. citizens, thereby creating a virtuous cycle of expertise between government and non-government experts. As many translated materials as possible should be made available in some form to the public.

With these attributes in mind, an open source entity could be organized in one of four broad ways, each with its own set of barriers and avenues to success.

1. New Open Source Information Agency (Non-Title 50 Entity)

An independent agency could be stood up within the executive branch, either as an independent office reporting to the White House or as an agency reporting to an existing department independent of existing IC elements. Potential departments include Commerce, Defense, State, or the General Services Administration. Federal statute, along with select agency and IC policies, would establish the roles, purpose, and responsibilities of the entity.

This agency should have an element that is a member of the IC in much the same way that the Department of State's Bureau of Intelligence and Research and the Department of the Treasury's Office of Intelligence and Analysis are members. If it were placed in the Department of Defense, this agency should function as part of the Military Intelligence Program and National Intelligence Programs, reporting to the Secretary of Defense and the Undersecretary of Defense for Intelligence.[108] This IC component would serve as a gateway between the new agency and the rest of the IC, facilitating the dissemination of open source products, structured data, and any other relevant products of the agency. This would ensure that open source has a voice within the IC – just like other intelligence disciplines. By being outside the IC, the agency would have greater independence to support relevant decision makers across the U.S. Government.

2. New Open Source Intelligence Agency (Title 50 Entity).

Congress, the White House, and the DNI could authorize, appropriate, and establish an independent open source intelligence agency as the nineteenth member of the IC. This agency would be the IC's functional manager and focal point for open source collection, analysis, and tradecraft with a mandate for and new resources to oversee collection and analysis to assist the IC, and the private sector, in defending against cyber-attack, espionage, and information warfare. As a pure, but standalone IC entity, this version of an open source center would be more tightly entwined with routine intelligence functions. Its entire workforce would be eligible for rotational assignments around the IC, ensuring that open source tradecraft and collection is better integrated in interagency task forces and analytic bodies like the

[108] 10 U.S.C. §137; 50 U.S.C. §3038.

National Intelligence Council. Standing up this agency, however, will require an amount of resources and authorities similar to those necessary for the operation of an open source information entity.

3. Coordination Office.

A coordination office within the Office of the Director of National Intelligence could also host open source collection function and information for the IC, deconflict the IC's open source activities, coordinate purchasing, licensing, and managing of commercial data for the U.S. Government, and serve as the point of contact on federal open source intelligence activities.[109] The foundation for such a network could build on existing IC coordination frameworks, namely ODNI's Federal Intelligence Coordination Office structure,[110] to provide objective, timely, accurate, and insightful open source intelligence responsive to the demands of decision makers *writ large*. In doing so, this entity would centralize open source data within the IC and demand less time and resources than a new independent entity otherwise would. At the same time, such a coordination office risks missing on building sustained expertise in the open source intelligence discipline because of its reliance on outsourced expertise and all-source analysts. Those analysts, whose expertise lies in a regional or functional specialty in supporting decisions, cannot replace the role of dedicated collectors.[111] Furthermore, the procurement and collection of publicly and commercially available information demands a cadre of professional collectors with both domain expertise and technical knowledge to discern credible sources from those that are not, and to communicate the necessary context as open source reports are disseminated for wider usage.

4. Normalize Open Source Use Across IC Analytic Units.

Rather than establishing a new entity, all U.S. government agencies – regardless of whether or not they have functions that fall under Title 50 jurisdiction – could adopt the methodical integration of open sources in greater quantities in all-source analysis and the creation of a set of standards when collecting, processing, and analyzing open source data. Although analytic training and tradecraft, review processes, and resources could be enhanced to address the U.S. Government's deficit in open source intelligence,[112] normalization of open sources for use among all-source analysts fails to account for the collection and processing challenge. Similar to how a coordination office fails to build a foundation of excellence upon which a future cohort of open source intelligence analysts could be drawn from, normalization depends on the assumption that existing analysts and institutions are willing and able to meet the demand of a competition in the digital age when in reality changing agency culture is a formidable challenge.

[109] Final Report, National Security Commission on Artificial Intelligence at 354 (2021).
[110] Intelligence Community Directive 404, U.S. Office of the Director of National Intelligence (2013).
[111] Hearing before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security, Using Open Source Information Effectively at 31 (2005).
[112] For another version of this argument, see Emily Harding, Move Over JARVIS, Meet OSCAR, Center for Strategic and International Studies (2022).

Options for Leveraging Open Source Capabilities

	Option 1: New Open Source Information Agency (Outside the IC)	**Option 2:** New Open Source Intelligence Agency (Within the IC)	**Option 3:** New ODNI Open Source Coordination Office (OSCO)	**Option 4:** Normalize Open Source Use Across IC Analytic Units
Brief Description	Establish an independent agency or office to carry out open source collection, analysis, and informational support for U.S. policymakers and the IC.	Establish an independent agency primarily responsible for the collection and analysis of open source intelligence.	Establish an office within the ODNI that would host open source information for the IC. OSCO would serve as the IC's focal point for open source contracting and processing.	Encourage the normalization of open source in the IC by creating an set of standards when collecting, processing, and analyzing open source data.
Institutional Location	Potential locations include: • Executive, Standalone Agency • Commerce, Independent Office • Defense, Independent Agency • State, Independent Office • GSA, Independent Office	19th Member of the Intelligence Community	ODNI	Across IC elements
Legal Authority to Access and Acquire Data	While this agency is not limited by Title 50 authorities, its collection activities will be governed by the existing or future statutory schemes consistent with the broad policy objectives of its host agency or branch.	This agency would be subject to Title 50's authorities. However, the DNI should further designate it as the IC agency responsible for the collection of open source intelligence within the Title 50 framework.	This office would be subject to Title 50's authorities. However, ODNI must also pursue blank purchase agreements within the 48 CFR § 8.405-3 framework.	Authorities would vary based on the agency implementing the policies.
Oversight and Accountability	Subject to congressional oversight by the relevant committees and/or jointly with SSCI & HPSCI, with any other form of oversight varying based on the selected host agency.	Subject to congressional committee oversight (SSCI & HPSCI). Additional interactions from governing board and an advisory committee.	Subject to congressional committee oversight (SSCI & HPSCI).	Subject to congressional committee oversight (SSCI & HPSCI), with any other form of oversight varying based on the agency.
Pros	• Lower barriers for entry with personnel, partnerships, and tech. • More likely to operate at lowest level of classification.	• Legitimizes open source intelligence as IC function. • Benefits from existing IC budget and infrastructure.	• Resolves the acquisition problem for commercially available data. • Centralizes publicly/ commercially available data within the IC.	• Intelligence agencies have autonomy to meet their own open source needs. • Requires no action from outside the IC.
Cons	• Limits potential impact on IC. • Institutional host may not prioritize the new agency.	• Requires significant adjustment of National Intelligence Program and Military Intelligence Program funding. • Must deconflict with existing open source systems.	• Retains the status quo for all-source analysis. • Relies on outsourced expertise.	• This is the status quo. • Open source collection and processing problems remain unresolved.

The U.S. Government must attempt to make as many open source products a utility available to all Americans, creating a virtuous cycle of expertise between government and non-government experts. Today's techno-economic competition demands a higher degree of shared knowledge and understanding across U.S. society. The opaque and controlled information environments of U.S. rivals, especially the PRC, require a high degree of knowledge to identify the authoritative signals that these governments publish for internal and external audiences. Americans should have access to a shared set of facts and reporting. Where the bounds of privacy and data licensing permit, the U.S. Government should aim for the broadest possible accessibility of open source translations and useful foreign data collections.

Publishing translated materials previously was a part of the open source mission. From the 1940s to 2013, when the service ended, IC open source experts helped curate and publish foreign media translations and analyses for public use.[113] U.S. academics, in turn, used these resources – often not readily available elsewhere – to shed light on important developments in the PRC and other closed societies, which subsequently informed U.S. policymakers.[114] The U.S. Government should recreate this service for an age of AI and emerging technologies. It must treat open source as a utility that enables the IC's ability to provide insight to Americans outside of government *and* harness insights from these Americans to inform policymakers.

Strengthening U.S. open source capabilities provides one of the best "use cases" for shifting the IC practices critical to mastering artificial intelligence. In strengthening open source, the IC could also make it into the leading "use case" for AI-enabled transformation because:

- The ability to transfer commercial AI approaches to open source problems would streamline its path to success and allow an open source entity to become operational and scale faster.

- The demand for open source intelligence is profound, and multiple agencies can leverage open source data for their own insights. Using AI would enable the curation and improved vetting of open source data at scale.

- The relative transparency of an open source agency would ensure that AI and emerging technologies achievements and lessons learned would remain visible to other individual agencies and help guide them in their own technology transformation. The current pedagogical approach of learning from intelligence failures and keeping successes secret is inadequate in the age of AI and emerging technologies.

The collective success demonstrated by these "use cases" will be a visible vehicle for guiding future IC projects. The more transparent environment of an open source agency would ensure that its AI achievements would remain visible to other individual agencies and help guide them in their own technology adoption and transformation. Open source's ability to transfer knowledge and lessons learned across the IC is one of its internal competitive advantages: it can be a mechanism for the dissemination of

[113] At the end of 2013, OSC shut down the subscription service, citing costs, the availability of alternative sources, and potential copyright issues. See Steven Aftergood, CIA Halts Public Access to Open Source Service, Federation of American Scientists (2013); Steven Aftergood, CIA Cuts Off Public Access to Its Translated News Reports, Federation of American Scientists (2014); Steven Aftergood, Open Source Center (OSC) Becomes Open Source Enterprise (OSE), Federation of American Scientists (2015).
[114] Gary Sick, Letter to Secretary of Commerce William Daley, (1999); SCSP Staff Engagement with Retired Intelligence Official (March 2022); Hal Brands, The Twilight Struggle: What the Cold War Teaches Us about Great-Power Rivalry Today, Yale University Press at 163-164 (2022).

knowledge about AI adoption. An AI-enabled open source agency has the potential to transform the entire IC culture into one that more strongly encourages speed of execution, experimentation, and collaboration: all the traits necessary to win the mid-decade competition.

Furthermore, the impact of achieving an AI-enabled open source intelligence capability could be significant and far-reaching. The potential importance and broad use of an open source agency's products and services by end consumers and other intelligence agencies underscores the urgent need for AI adoption. However, AI adoption itself is not the end goal, but merely the means for capturing insight. Other agencies would be able to leverage a common open source data repository to create their own insights. The scaling of AI would allow an open source agency to curate open source data: to vet, classify, and tag it for reliability. This could translate into a more sophisticated use of intelligence and a stronger awareness of sourcing by consumers which could then improve their use of analysis derived from exquisite collection.

An open source agency could also accelerate the training of AI models that other IC agencies might use by "pre-training" models in common domains over its large collection of open source data. AI could also transform intelligence dissemination and policymaker support by enabling the creation of custom machine learning (ML)-written open source digests or daily summaries tailored to the individual needs of policymakers and analysts. The ability to collect, curate, and compress this vast volume of information could also be combined with AI's ability to deliver intelligence in new ways, to present intelligence in bespoke audio or visual formats, instead of text, to meet the individual preferences of decision makers.

Creating Techno-Economic Intelligence

The IC is transitioning toward the Administration's policy statement that "economic security is national security."[115] The PRC is an all-encompassing strategic rival that challenges the United States across industry, finance, and technology.[116] Consequently, U.S. intelligence must reorganize and retool for economic competition in order to defend Americans' standard-of-living, support a U.S. Techno-Industrial Strategy,[117] and protect the interests of the United States and its allies around the world.

The economic competition with the PRC is wide in scope and fierce in intensity. The PRC's gross domestic product (GDP) in market terms is nearing that of the United States.[118] Although it is well-recognized that the PRC has used state-sponsored programs to steal U.S intellectual property,[119] it has also invested significantly in critical technologies, such as artificial intelligence, with the goal of being the world leader in AI by 2030.[120] The PRC still champions the installation of ZTE and Huawei's 5G systems around the

[115] Interim National Security Strategic Guidance, The White House at 15 (2021).
[116] Graham Allison, et al., The Great Economic Rivalry: China vs the U.S., Belfer Center for Science and International Affairs (2022); Emily de La Bruyère & Nathan Picarsic, Elemental Strategy: Countering the Chinese Communist Party's Efforts to Dominate the Rare Earth Industry, Foundation for the Defense of Democracies (2022); Phelim Kline, China's Long Shadow Looms Over Biden's Americas Summit, Politico (2022); Final Report, National Security Commission on Artificial Intelligence (2021).
[117] Mid-Decade Challenges to National Competitiveness, Special Competitive Studies Project at 55 - 81 (2022).
[118] The Great Economic Rivalry: China vs the U.S., Belfer Center for Science and International Affairs (2022).
[119] Remarks by FBI Director Wray on The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States, U.S. Federal Bureau of Investigation (2020). For a detailed example of these PRC efforts, see Jordan Robertson & Drake Bennett, A Chinese Spy Wanted GE's Secrets, But the US Got China's Instead, Bloomberg Businessweek (2022).
[120] Final Report, National Security Commission on Artificial Intelligence at 160 (2021).

globe,[121] and has promoted more than 1,500 physical and digital infrastructure projects globally through the Belt and Road Initiative.[122] The PRC's ties reach deeply into the Western hemisphere, as it is now the leading trade partner with South America.[123]

The PRC's national strategy of military-civil fusion,[124] through which it integrates its civilian economy with its military industrial base, also means that this economic competition carries directly over into traditional national security areas. These conditions require U.S. intelligence to strengthen its techno-economic intelligence capabilities, to be able to peek under the hood of the PRC's economy and to have a detailed understanding of the CCP's industrial and technological priorities and pursuits. This includes the PRC's trade behavior, key industries and companies, critical supply chains, and investment flows. U.S. intelligence will also need to understand the PRC's emerging platforms in technology and finance, especially as these data-collecting, strategic platforms are exported abroad.[125]

U.S. policymakers are making increasing use of financial and economic tools of statecraft for geopolitical aims. Following the invasion of Ukraine, the United States and its allies have imposed more than 12,000 sanctions on individuals, entities, vessels and aircraft connected with Russia.[126] The use of these wide-ranging sanctions requires continually assessing their costs and benefits, tracking global compliance, and identifying possible future targets.[127] Understanding the impact of these actions, such as the freezing of Russia's central bank reserves or the embargo of its energy exports, on the United States' economy and the overall world economy is needed to assess their full costs and benefits.

U.S. intelligence should leverage insights from the private sector to improve the picture of U.S. adversaries' economic, financial, and technological capabilities. U.S. intelligence should leverage, not recreate, the private sector's collection and analysis of economic information. Forming public-private partnerships with industry, Wall Street banks, consulting firms, academia, and the business media would enable U.S. intelligence to efficiently build upon their sector expertise, broader resources, on the ground presence, and market-based insights, and marry it with IC information to create a more comprehensive "all-source" intelligence picture.

Existing government economic intelligence efforts are often tightly aligned with departmental missions, where organizational and technological constraints hinder the creation of an integrated picture of U.S. economic security. A full-spectrum adversary challenging the United States in every domain requires this integrated assessment. The CIA produces economic intelligence, but security concerns limit its ability to partner with external providers. The Department of Treasury's efforts focus heavily on combating illicit financing, whereas elements of the U.S. Federal Statistical System such as the Bureau of Economic Analysis within the Department of Commerce aim to supply domestically-oriented data for government and public uses.

[121] Stefan Pongratz 1Q22 Total Telecom Equipment Market: ZTE Gains Share Dell'Oro Group (2022).
[122] Mapping the Belt and Road Initiative, Mercator Institute for China Studies (last accessed 2022).
[123] Phelim Kline, China's Long Shadow Looms Over Biden's Americas Summit, Politico (2022).
[124] Military-Civil Fusion and the People's Republic of China, U.S. Department of State (2020).
[125] Emily de La Bruyère, et al., China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order, The National Bureau of Asian Research (2022).
[126] Russia Sanctions Dashboard, Castellum.ai (last accessed 2022).
[127] An initial effort in this regard is the Department of Treasury's new office to research the unintended consequences of economic spillover. See Daniel Flatley, Now Hiring: US Seeks Economist to Scrutinize Sanction Spillovers, Bloomberg (2022).

In assessing the various options, policymakers should note that an entity that could effectively lead U.S. national techno-economic intelligence needs the following characteristics:

- ***Gateway*.** A new entity should act as a gateway for integrating economic and industry data already collected by Commerce with U.S. intelligence reporting to produce sector-specific techno-economic threat intelligence for industry and policymakers.

- ***AI-enabled Tools and Platforms.*** A new entity should have the capacity and technical expertise to build and maintain an "all-source" AI-enabled "techno-economic dashboard." This tool would capture critical techno-economic threats from foreign industries, supply chains, and individual companies in near real-time to provide preemptive and predictive insights – from the macroeconomic level down to the individual company.

- ***Dissemination.*** A new entity should have the authority to disseminate insights from the techno-economic dashboard to a broad range of stakeholders to, for instance, inform economic aspects of U.S. Government wargames and tabletop exercises for economic policy decisions. These insights must include forecasts about reactions to, and second-order implications of, U.S. policies, ranging from sanctions targeting, to choices about reshoring and friendshoring

- ***Connections.*** A new entity should liaise between the IC and national security-related programs within the Department of Commerce like the Strategic Intelligence Division under the Bureau of Industry and Security (BIS).

- ***Standards*.** An entity should uphold the standards outlined in the Department of Commerce's 2021-2024 Data Strategy, including the implementation of an ethical data lifecycle that protects privacy, respects intellectual property, addresses cybersecurity concerns, and fosters an ethical data lifecycle that minimizes algorithmic risk of unintended bias.[128]

The U.S. Government should establish a National Techno-Economic Intelligence Center to capture, master, and disseminate economic, financial, and technological intelligence. This National Techno-Economic Intelligence Center should coordinate economic threat information and work closely with policymakers on responses to these threats.[129] The center should be established under a well-resourced sponsor that can support its mandate within the U.S. Government. Using AI to collect and process economic information at scale, this economic "nerve center" would be able to make economic assessments and forecasts, as well as fuel innovation in economic modeling. This center, with analysts trained for techno-economic analysis, would warn of foreign threats to the U.S. economy, make sense of rivals' grand strategies,[130] apprise the U.S. industry about threats such as intellectual property theft and supply chain vulnerabilities, and evaluate opportunities to deploy tools of economic leverage.

At a minimum, the Department of Commerce, in particular, should expand its techno-economic intelligence capabilities and set up an office responsible for integrating economic and industry data already collected by Commerce with U.S. intelligence reporting to produce sector-specific techno-

[128] Commerce Data Strategy: Fiscal Years 2021-2024, U.S. Department of Commerce (2021).
[129] Anthony Vinci, Competitive Climate: America Must Counter China by Investing in Economic Intelligence, National Interest (2020); John Costello, et al., From Plan to Action: Operationalizing a U.S. National Technology Strategy, Center for a New American Security (2021).
[130] Rush Doshi, The Long Game: China's Grand Strategy to Displace American Order, Oxford University Press (2021).

economic threat intelligence for industry and policymakers, while ensuring the necessary safeguards to protect the privacy of American citizens and the proprietary information of U.S. companies.

Options for a National Techno-Economic Intelligence Center[131]

	Option 1: New Techno-Economic Information Center (Outside the IC)	**Option 2:** New Commerce Techno-Economic Intelligence Office (Within the IC)	**Option 3:** New ODNI National Techno-Economic Intelligence Center	**Option 4:** Expanded CIA Mission Center on Techno-Economic Intelligence
Brief Description	Establish an independent agency or office to conduct techno-economic analysis.	Establish an IC element within Commerce responsible for collecting, analyzing, and disseminating foreign techno-economic intelligence.	Establish a national "nerve center" within ODNI responsible for collecting, analyzing, and disseminating techno-economic intelligence across the IC.	Expand the scope of the CIA's Transnational and Technology Mission Center (T2MC).
Institutional Location	Executive Agency	Commerce	ODNI	CIA
Legal Authority to Access and Acquire Data	This entity would NOT be subject to Title 50 authorities. Subject to the Privacy Act of 1974.	This entity would be subject to Title 50 authorities and may need new authorities to make full use of Commerce's data.	This entity would be subject to Title 50 authorities and may need new authorities for data access and net assessments.	This entity would be subject to Title 50 authorities and may need new authorities for data access and net assessments.
Oversight and Accountability	Potentially subject to relevant congressional oversight bodies.	Subject to congressional oversight (SSCI & HPSCI).	Subject to congressional oversight (SSCI & HPSCI).	Subject to congressional oversight (SSCI & HPSCI).
Pros	• A standalone entity would have the most flexibility and individual drive of the options. • Public trust in the entity may be higher as a non-Title 50 entity.	• Maintaining the entity within Commerce may ease flow of data and intelligence concerns. • The proposed purpose of this entity most aligns with Commerce's authorities.	• ODNI is well-positioned to coordinate and host such an interagency entity. • Oversight authorities and existing precedent for a coordination center are clear.	• Expanding existing mission guidelines may be quicker. • CIA already has many of the resources, personnel, and authorities necessary for the expanded mission.
Cons	• An information center outside the IC would not benefit from existing IC infrastructure and procedures for policy support.	• Having an IC entity within Commerce might detract from the department's main purpose. • Commerce might not be a strong sponsor within the IC.	• ODNI would need more resources to independently support such a center. • May be subject to existing classification concerns.	• May not be able to utilize all the economic intelligence that Commerce gathers given siloing. • Restricted remit.

[131] The success of these organizational options also depends on the simultaneous adoption of the other recommendations in this section. These recommendations are intended to build on each other to best position the IC and U.S. Government for competitive advantage in the techno-economic competition.

This type of intelligence should be disseminated to a wide range of U.S. Government consumers who work on national techno-economic competitiveness. The center should also develop a mechanism or outreach network to raise the awareness of U.S. companies about critical sector threats in their competitive space as part of protecting U.S. interests and enabling better corporate risk management.

U.S. intelligence should create a new techno-economic analyst career track to evaluate foreign corporations, their technological developments, critical supply chains, and broader macroeconomic activity. In order to produce economic intelligence on industries, technologies, companies, and critical supply chains, U.S. intelligence will need analysts with skills similar to those of analysts working within U.S. financial services, consulting firms, and private industry. Investment banks hire university graduates and use two- to three-month intensive training programs to provide them with the foundation of skills needed for their careers.[132] U.S. intelligence should look at these programs as potential models for training techno-economic analysts, which would become a new occupational series that would have a crucial role in producing data-driven, corporate-intensive, techno-economic intelligence.

Revamped retention and compensation practices will be needed to maintain this techno-economic analytical capability within U.S. intelligence over the long-term. It will be necessary to change policies and cultural norms to allow highly trained personnel to leave U.S. intelligence and return later with career opportunities that remain undiminished for these periods outside government. This flexibility is needed because U.S. intelligence cannot compete on compensation alone.[133] External positions should be viewed as giving intelligence personnel prized work experience that they can later use to better understand industries, companies, and technologies for the U.S. Government.

Existing departments should augment their in-house intelligence elements to strengthen their techno-economic capabilities and better inform U.S. entities about adversarial threats. U.S. departments and agencies should create or augment, as the case may be, in-house intelligence elements to ensure that the IC and our recommended National Techno-Economic Intelligence Center have all available knowledge. Such augmentation could include secondments from the recommended center, dual-hatting the center's analysts in these departments, or the creation of interagency teams. In some instances, this will also require expanded collection mandates. These intelligence elements should be structured to allow these Departments to maintain their existing and important roles as open-door vehicles for private industry to engage the U.S. government on informational, regulatory, or other administrative matters.

The Department of Commerce should expand its techno-economic intelligence capabilities and enrich technical, economic, and industry data already collected by Commerce with U.S. intelligence reporting to produce sector specific techno-economic threat intelligence – while ensuring all the necessary privacy safeguards for American citizens. It should also proactively disseminate threat briefings to U.S. companies in critical industries. In a similar way that Cybersecurity and Infrastructure Security Agency (CISA) briefs U.S. companies on cyber threats,[134] Commerce should alert companies to specific threat vectors such as state-sponsored economic espionage. These threat briefings should be structured to include a two-way

[132] Mary Biekert, Wall Street's Hottest Commodity: College Grads With Excel Skills, Bloomberg (2022).
[133] The salaries for first-, second-, and third-year analysts in the financial sector have roughly equivalent compensation to that of GS-13 and GS-14 U.S. officials living in the Washington Metropolitan Area. See Tom Metcalf, JP Morgan Raises Salaries for Junior Bankers for Second Time, Bloomberg (2022); 2022 General Schedule (GS) Locality Pay Tables, U.S. Office of Personnel Management (2022).
[134] Information Sharing and Awareness, U.S. Cybersecurity & Infrastructure Security Agency (last accessed 2022).

information flow that allows Commerce to educate industry on economic threats and share pertinent information with the IC.

U.S. intelligence needs the authorities, capabilities, and incentives to make techno-economic net assessments. The IC should be able to provide policymakers with an economic "order of battle" for our strategic rivals that maps out and details critical supply chains, technologies, industries, and companies. The deep interconnections between the PRC and the United States through global trade and finance means that it will be essential for U.S. intelligence to have the ability to do complex analysis involving U.S. companies. For this, the IC, or select elements within it, needs the authority and internal guidelines to conduct these net assessments while ensuring appropriate privacy safeguards for U.S. citizens. It should prioritize supporting other government centers tasked with providing technology net assessments, such as the Office of Global Technology Competition Analysis proposed by the American Technology leadership Act or a Technology Competitiveness Council (TCC), proposed by the NSCAI and highlighted in SCSP's Mid-Decade Challenges to National Competitiveness.[135]

U.S. intelligence collection should include adversary scientific and technological research that has dual-use purpose or application. The United States has enjoyed the position as the world's dominant economic and technological power since World War II,[136] reducing somewhat the need for IC awareness of adversarial scientific and technological research. However, growing research on dual-use technologies and their application by U.S. adversaries that leverages innovations across military and civilian sectors requires the IC to expand its awareness.[137]

The PRC's domestic innovation base[138] should be considered a U.S. intelligence collection priority. These technological advancements should be seen as growing target opportunities by U.S. intelligence to protect and inform our own, government-led scientific and technological research efforts.

Countering Foreign Adversarial Influence Operations

While the concept of foreign influence itself is not new, there are recent, notable changes to the venues and vectors through which it is being deployed. Technological advancements and the emergence of new media platforms have enhanced the speed, reach, volume, and precision of disinformation generated by foreign adversaries. U.S. rivals increasingly resort to the aggressive use of digitally-enabled disinformation to target U.S. decision-making, America's reputation abroad, and social cohesion at home. Trolls, bots, and deepfakes employed by the PRC's cyber militias and Russia's Internet Research Agency are also aiming

[135] In 2022, Congress considered legislation for both a Technology Competitiveness Council (TCC) and Office of Global Competition Analysis (OCA). H.R. 8027, To Establish within the Executive Office of the President a Technology Competitiveness Council (2022); Courtney Albon, Lawmakers Propose 'Technology Competitiveness Council' to Champion US Innovation, C4ISRNet (2022); S. 4368, American Technology Leadership Act of 2022 (2022); Daniel Flatley, Senators Wary of China's Tech Prowess Seek Competition Office, Bloomberg (2022). The NSCAI recommended creating a TCC in its final report in 2021. Final Report, National Security Commission on Artificial Intelligence at 166 (2021).

[136] Fareed Zakaria, The Future of American Power: How America Can Survive the Rise of the Rest, Foreign Affairs (2008).

[137] Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, Office of the Secretary of Defense at IV (2021).

[138] Emily Weinstein, Beijing's 'Re-innovation' Strategy is Key Element of U.S.-China Competition, Brookings (2022).

to erode key tenets of democracy until people question what is demonstrably true.[139] The scale, scope, and the snowballing effect of these influence operations make disinformation a particularly acute concern for national security.

To uphold the 2022 National Security Strategy's declaration that the United States is "standing up to threats to our democracy" including "information manipulation operations,"[140] the U.S. Government must protect Americans from, counter the effects of, and disrupt adversary influence operations. There will be no one size fits all solution to countering this problem, but rather a series of partial solutions coming together.[141]

[139] Katerina Sedova, et al., AI and the Future of Disinformation Campaigns Part 1: The RICHDATA Framework, Georgetown University, Center for Security and Emerging Technology (2021); Katerina Sedova, et al., AI and the Future of Disinformation Campaigns Part 2: A Threat Model, Georgetown University, Center for Security and Emerging Technology (2021).
[140] The National Security Strategy of the United States, The White House at 16 (2022).
[141] Sylvia Burwell, Future of Democracy, Global Emerging Technology Summit, Special Competitive Studies Project at 26:47 (2022).

Disinformation

"Content that is intentionally false and designed to cause harm."[142]

Misinformation

"False content, but the person sharing doesn't realize that it is false or misleading." [143]

Malinformation

"Genuine information that is shared with an intent to cause harm." [144]

Influence Operation

"Organized attempts to achieve a specific effect among a target audience." [145]

Information Campaign

State directed, or otherwise sponsored, efforts that employ information "intended to generate specific outcomes or effects in a relatively large number of individuals, usually within a specified period of time, and through an organized set of communication activities." [146]

[142] Claire Wardle, Understanding Information Disorder, First Draft News (2020).
[143] Claire Wardle, Understanding Information Disorder, First Draft News (2020).
[144] Claire Wardle, Understanding Information Disorder, First Draft News (2020).
[145] Elise Thomas, et al., The Challenges of Countering Influence Operations, Carnegie Endowment for International Peace (2020).
[146] Everett M. Rogers & Douglas Storey, Communication Campaigns, Sage at 821 (1987).

The Intelligence Community should continue to prioritize countering foreign adversarial influence operations. To do so more effectively, the U.S. Government should operationalize the Foreign Malign Influence Response Center alongside a Joint Interagency Task Force (JIATF) and Operations Center. The U.S. Government engages in countering foreign adversarial influence operations through several efforts. They include, but are not limited to: the Federal Bureau of Investigation's Foreign Influence Task Force (FTIF),[147] the United State Cyber Command,[148] Cybersecurity and Infrastructure Agency's Mis-, Dis-, and Malinformation Team,[149] the Office of the Director of National Intelligence's Election Threat Executive,[150] and the Department of State's Global Engagement Center (GEC).[151]

Outside of the U.S. Government, entities ranging from private companies to government agencies coordinate with each other to improve information sharing about these threats. The Five Eyes[152] and G-7 Media Ministers, for example, work to counter disinformation.[153] The 2021 National Defense Authorization Act also authorized an Information Sharing and Analysis Center (ISAC) titled "Social Media Data and Threat Analysis Center" to encourage defense industrial base entities to cooperate with private social media company ISACs where appropriate, to counter disinformation online.[154]

Most recently, Congress authorized the Foreign Malign Influence Response Center to serve as a coordinating body under ODNI,[155] and the associated Foreign Malign Influence Coordinator position on the National Security Council.[156] The center initially received widespread support, but has since been delayed due to resource concerns.[157] The NSCAI affirmed the importance of the Foreign Malign Influence Response Center to coordinate countering influence campaigns, and additionally recommended the creation of a JIATF and Operations Center.[158]

While the status and scope of these efforts vary, the need for an IC leader to coordinate with internal and external actors, working across the cyber and information domains, to counter foreign disinformation remains constant. Foreign adversaries are continually targeting the United States with disinformation campaigns while the United States struggles to adopt a coordinated response. Some U.S. policymakers have even expressed that the Foreign Malign Influence Response Center, Foreign Malign Influence Coordinator, and Information Sharing and Analysis Center are necessary authorizations for strengthening U.S. capabilities in this domain.[159] We recommend operationalizing the Foreign Malign Influence Response Center to act as a centralized point of contact for collaboration between the various U.S. Government agencies and external entities to counter foreign adversarial influence operations affecting the democratic society within the United States, and among allies and partners. Simultaneously, the White House should

[147] Combating Foreign Influence, U.S. Federal Bureau of Investigation (last accessed 2022).
[148] Mission and Vision, U.S. Cyber Command (last accessed 2022).
[149] Mis-, Dis-, Malinformation, U.S. Cybersecurity and Infrastructure Security Agency (last accessed 2022).
[150] Election Security - Who We Are, Office of the Director of National Intelligence (last accessed 2022).
[151] Global Engagement Center, U.S. Department of State (last accessed 2022). The Disinfo Cloud, formerly associated with GEC, is an example of a U.S. Government initiative to counter disinformation through collaborative efforts. See Tackling Propaganda and Disinformation, Disinfo Cloud (2022).
[152] Home Secretary Meeting with 'Five Eyes' Counterparts, Government of the United Kingdom (2022).
[153] Combating Disinformation and Supporting Freedom of the Press, G7 Germany (2022).
[154] Public Law 116-92, National Defense Authorization Act for Fiscal Year 2020, § 5323 (2019); Public Law 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, § 9301 (2020).
[155] 50 USC § 3059 (2021).
[156] Pub. L. 115-232, John S. McCain National Defense Authorization Act for Fiscal Year 2019, § 1043(g) (2018).
[157] Nomaan Merchant, US Delays Intelligence Center Targeting Foreign Influence, Federal News Network (2022).
[158] Final Report, National Security Commission on Artificial Intelligence at 48, 274 (2021).
[159] Amy Klobuchar, Jack Reed, & Gary C. Peters, Untitled Letter on Countering Malign Foreign Influence Campaigns (2021).

take steps to follow through on the NSCAI's recommendation to create a JIATF and Operations Center. The JIATF and Operations Center could use the Congressionally-approved authorities awarded to the Foreign Malign Influence Response Center and improve upon it by building out a technologically-enabled operations center as detailed in the NSCAI Final Report.[160]

The U.S. Government – including the Intelligence Community – should aim to preemptively counter foreign adversarial influence operations. Prior to Russia's invasion of Ukraine, the United States and the United Kingdom engaged in what appears to have been deliberate disclosure and exposure of Russian malign intentions.[161] This approach should be replicated whenever possible and suitable. Through early disclosures of anticipated malign actions, U.S. and allied governments could potentially deter or, at a minimum, "prebunk" them.[162] The "prebunking" could help raise awareness among the domestic public, enabling them to sense and avoid misleading content proliferating in their newsfeeds.[163] By providing the public with the information they need to protect themselves against misleading or false narratives and information, prebunking provides nation-wide protection.

[160] Final Report, National Security Commission on Artificial Intelligence at 48, 274-276 (2021).
[161] Jessica Brandt, Preempting Putin: Washington's Campaign of Intelligence Disclosures is Complicating Moscow's Plans for Ukraine, Brookings (2022); Douglas London, To Reveal, or Not to Reveal: The Calculus Behind U.S. Intelligence Disclosures, Foreign Affairs (2022).
[162] Laura Garcia & Tommy Shane, A Guide to Prebunking: A Promising Way to Inoculate Against Misinformation, First Draft (2021).
[163] Jon Roozenbeel, et al., Prebunking Interventions Based on "Inoculation" Theory Can Reduce Susceptibility to Misinformation Across Cultures, Harvard Kennedy School Misinformation Review (2020); Jonas De keersmaecker & Arne Roets, "Fake News": Incorrect, but Hard to Correct. The Role of Cognitive Ability on the Impact of False Information on Social Impressions, Intelligence at 65, 107–110 (2017).

[164] Laura Garcia & Tommy Shane, A Guide to Prebunking: A Promising Way to Inoculate Against Misinformation, First Draft News (2021).
[165] Fact-Checking and Debunking: A Best Practice Guide to Dealing with Disinformation, NATO Strategic Communications Center of Excellence (2021).

The U.S. Government should warn of foreign-backed disinformation as part of its early-stage countermeasures. "Prebunking" disclosures may not be always possible.[166] Therefore, the U.S. Government should also aim to alert the public of foreign influence operations already underway that seek to undermine the social cohesion of the United States. While such foreign disinformation operations may not have an obvious tactical urgency, they can have strategic consequences. The IC could collaborate on this endeavor with the CISA and expand the National Cyber Awareness System[167] to alert the public about foreign disinformation operations of strategic import.

Create a public notice board of adversary-generated false narratives and themes to expose them and encourage public research. Not all foreign disinformation will be strategically consequential. And the U.S. government will be hard pressed to counter it all. In such instances, the U.S. government could publicly identify false narratives and themes propagated by U.S. adversaries that aim at the truth more broadly and at U.S. reputation abroad. This publicizing could then enable the private sector and academic researchers to examine them further. Entities such as University of Washington's Center for an Informed Public, Stanford's Internet Observatory, and the Atlantic Council's Digital Forensic Research lab are examples of existing independent expertise that could be a force multiplier for this resource-demanding mission.[168]

Designate a focal point that tracks and counters foreign-directed denigration campaigns against senior U.S. leaders. Our adversaries are working to acquire, analyze, and weaponize data on DNA, dating preferences, shopping tendencies, social networking, and professional experiences of much of the U.S. population.[169] Empowered by AI, this trend could allow foreign intelligence services to micro-target senior civilian and military leaders by denigrating them in the public domain and orchestrating character assassination efforts.[170] Such micro-targeting could put senior U.S. leaders under considerable pressure and distract them from discharging their duties. For example, after U.S. Department of State official Julie Eadeh was photographed in a room alongside Hong Kong protesters, the photo circulated among PRC state media, resulting in the release of her family's personal data on PRC chat and web sites, stalking, and the creation of a character in her likeness in a state-backed video game to "hunt down traitors who seek to separate Hong Kong from China."[171] Julie Eadeh's story is a public example of an increasingly dangerous trend among adversaries to employ denigration campaigns against U.S. officials by exploiting data to exacerbate the reach of such campaigns.

---

[166] Simge Andi & Jesper Akesson, Nudging Away False News: Evidence from a Social Norms Experiment, Digital Journalism at 121 (2020).

[167] National Cyber Awareness System, U.S. Cybersecurity & Infrastructure Security Agency (last accessed 2022).

[168] Center for an Informed Public, University of Washington (last accessed 2022); Internet Observatory, Stanford Cyber Policy Center (last accessed 2022); Digital Forensic Research Lab, Atlantic Council (last accessed 2022).

[169] For further discussion on individualized micro targeting, see Chapter 5 of Mid-Decade Challenges to National Competitiveness, Special Competitive Studies Project (2022).

[170] One example abroad is the targeting of U.S. Foreign Service Officer Julie Eadeh in Hong Kong. Timothy McLaughlin, How China Weaponized the Press, The Atlantic (2021). Note that micro-targeting is not limited to senior government civilian and military leaders, and also applies to kinetic attacks. For further discussion on micro targeting and individualization, see Mid-Decade Challenges to National Competitiveness, Special Competitive Studies Project at 126-127 (2022).

[171] Timothy McLaughlin, How China Weaponized the Press, The Atlantic (2021); David Brunnstorm, Chinese Reports on U.S. Diplomat in Hong Kong 'Have Gone From Irresponsible to Dangerous': State Department, Reuters (2019).

At present, it appears that no entity in the U.S. Government is specifically designated and resourced to track, counter, and disrupt such denigration efforts – and the collection efforts that support them. Even the Foreign Malign Influence Response Center emphasized above would not have the full capabilities to track and investigate denigration campaigns as currently written.[172] While further analysis of authorities and broader engagement of various stakeholders is required to recommend an institutional home, the imperative for designating an entity that focuses on this mission is already here. Key considerations for such an institutional home must address authorities related to the information domain, defining domestic versus international information space, and countering disinformation while respecting civil liberties and privacy, among other legal considerations.

The constant evolution of influence operations requires the Intelligence Community – and U.S. Government writ large – to incorporate new technologies and mitigation techniques quickly. Digital influence operations advance at an exponential rate, presenting the IC with the challenge of keeping pace.[173] Leveraging tools like the content provenance standards of the Coalition for Content Provenance and Authenticity[174] and DeepMind's RETRO database[175] could help the IC outpace adversaries by authenticating content origins and verifying information, respectfully, while embracing high speed human-machine teaming would increase overall speed of IC operations.[176] Researchers and officials could also train Large Language Models (LLMs) to identify classifiers of dangerous or harmful texts in strategic languages to identify threats to U.S. interests, and those of allies and partners, in multiple information domains.

Especially in the realm of content authentication and provenance, new technologies are critical. Recently, the NSCAI Final Report called for the creation of a "task force to study the use of AI and complementary technologies, including the development and deployment of standards and technologies, for certifying content authenticity and provenance."[177] Continuing to prioritize efforts in this realm will be central to combatting technologically-enabled foreign adversarial influence operations and disinformation. Bolstering digital literacy and societal resilience through other means, which is well-documented by other experts, remains necessary to countering adversarial influence.

[172] 50 USC § 3059 (2021).
[173] Examples of recent developments include AI-enabled autonomous disinformation, texts produced by large language models, and realistic images produced by systems like DALL-E 2, OpenAI (last accessed 2022).
[174] C2PA Specifications, Coalition for Content Provenance and Authenticity (last accessed 2022).
[175] Will Douglas Heaven, DeepMind Says Its New Language Model Can Beat Others 25 Times Its Size, MIT Technology Review (2021).
[176] For further discussion of Human-Machine Teaming, see Mid-Decade Challenges to National Competitiveness, Special Competitive Studies Project at 122-144 (2022); Defense Interim Panel Report, Special Competitive Studies Project at 26-33 (2022).
[177] Final Report, National Security Commission on Artificial Intelligence at 49 (2021).

Winning the Accelerating Race for Actionable Insight to Enable U.S. Statecraft

7 Ways to Adapt
IC Elements to the Technological Era and Rivalry through Digital Transformation

1. Drive reforms from the leadership level that unlock the IC's potential for digital transformation.
2. Ensure the right combination of people, processes, and technology.
3. Convene IC stakeholders to establish new standards for acceptable risks in digital transformation.
4. Set new security goals for the safe, secure integration of needed expertise and technology.
5. Modernize hiring, retention, and exchange policies to ensure access to needed expertise.
6. Learn from other large, complex organizations, but tailor to the IC's specialized mission.
7. Sponsor a Digital Experimentation and Transformation Unit to run pilot projects to resolve key problems for digital transformation.

6 Ways to Leverage
Insights and Information through Open Source Capabilities

1. Emphasize the collection and processing of public and commercial information at the core of expanded U.S. Government open source efforts.
2. Create a new, well-resourced institutional home for open source collection, acquisition, processing, and analysis.
3. Enable the new entity to serve as a gateway for open source data and analysis between the IC, U.S. Government, and external actors.
4. Leverage open source successes to spotlight best "use cases" for scaling AI across the IC.
5. Run a series of internal pilot projects to build skills in exploiting open sources with AI tools.
6. Publish select open source products to create a virtuous cycle of collaboration with non-government experts.

6 Ways to Create
New Capacities to Capture and Master Techno Economic Intelligence

1. Leverage private sector insights of adversaries' economic, financial, and technological capabilities.
2. Launch a National Techno-Economic Intelligence Center.
3. Design a new techno-economic analyst career track.
4. Augment in-house intelligence elements in existing departments to strengthen their techno-economic capabilities.
5. Establish the authorities, capabilities, and incentives to make techno-economic net assessments.
6. Prioritize collection on adversaries' scientific and technological research that has dual-use purpose or application.

6 Ways to Counter
Foreign Adversarial Influence Operations

1. Operationalize the Foreign Malign Influence Response Center alongside a Joint Interagency Task Force (JIATF) and Operations Center.
2. "Prebunk" foreign adversarial influence operations through early public disclosures.
3. Alert of foreign disinformation operations that target U.S. social cohesion.
4. Build a public notice board of adversary-generated false narratives and themes.
5. Designate a focal point to counter foreign denigration efforts against senior U.S. leaders.
6. Incorporate new technologies and mitigation techniques quickly.

SCSP.AI