Memos to the PRESIDENT

Intelligence Community (IC)

Special Competitive Studies Project

Memos to the
PRESIDENT

Subject: Reimagining U.S. Intelligence for the AI Age

Purpose: This memorandum outlines a set of ambitious goals for reforming the U.S. Intelligence Community (IC) that, if achieved, would position the IC to adapt to the coming wave of revolutionary technological change and improve its ability to protect the nation's economic competitiveness in the decades ahead.

Objectives: Given the IC's crucial role in securing the homeland and supporting the United States' ability to pursue its strategic goals, it must revolutionize its approach to its work and better address the importance of national techno-economic competitiveness. In doing so, it should reorient itself to fulfill five objectives:

1. *Elevate* the collection and analysis of foreign technology capabilities and economic threats to a top priority;
2. *Establish* a new and fully funded institutional home for Open Source Intelligence;
3. *Prioritize* the formation of strategic intelligence alliances to dominate the techno-economic advantage;
4. *Provide* the President with the means to push back against hybrid warfare threats; and
5. *Transform* the future IC workforce.

Problem Statement

The United States has entered a new era of profound transformation unprecedented in its history. Driven by artificial intelligence (AI) and associated emerging technologies, this new era will fundamentally change not only the range of global threats the IC must follow but also the capabilities it uses for detecting and assessing them. Along with this technological transformation, the IC faces a much more dynamic, uncertain, and dangerous geostrategic landscape marked by intensified techno-economic competition, more frequent and potentially destabilizing regional conflicts, more pervasive and economically damaging cyber and ransomware threats, and unprecedented levels of espionage and "gray zone" sabotage threats from the Axis of Disruptors: Russia, China, Iran, and North Korea. The IC must maintain vigilance and capabilities to deal with legacy threats, such as from still-lethal terrorist organizations, but urgently needs

to rebalance its priorities to focus on ensuring that the United States prevails in the looming techno-economic competition with the People's Republic of China (PRC).

Through all of this, the core missions of the IC remain unchanged: to provide U.S. leaders decision-making advantage over adversaries and competitors, and to expand the menu of options for the President. Whether or not the IC can fulfill its missions will depend critically on how fast it adapts to these new technological and geostrategic realities to sharpen its focus on key priorities and to implement necessary reforms to enhance speed and efficiency. Many of the IC's existing practices and organizational structures were purpose-built for the Cold War (and later adapted to the War on Terror) but are ill-suited for the fast-paced, technology-driven, "whole of nation" struggle in which all sectors of our economy and society are potential targets for disruption by the PRC and other adversaries.

The need for urgency is clear. U.S. intelligence services are already falling behind and are not moving fast enough to adopt AI and other key new technologies. As a consequence, they are losing ground to counterparts in China, Israel, and elsewhere. The IC is in serious danger of becoming irrelevant to U.S. decisionmakers who are able to access a wide array of openly-available sources for timely and insightful collection and analysis. The IC must adapt and learn to harness our nation's source of strength to deliver insights to policymakers at the speed of today's world.

Recommendations

What is needed is nothing short of a "Revolution in Intelligence Affairs"[1] to reverse these trends and set the IC on a course for continued long-term success. The IC's mission needs to be refocused on helping the United States and its allies win against the Axis of Disruptors. The incoming leaders of the U.S. Intelligence Community – with the backing of the White House and Congress – need to challenge existing paradigms and ways of doing business, push the IC to be more ambitious and daring, and lean into taking advantage of the rapid pace of technological change. To set the IC on a path toward success, we urge the Trump administration's national security team to establish five goals for U.S. Intelligence:

Objective 1: Elevate the collection and analysis of foreign technology capabilities and economic threats to a top priority.

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, and military domains to reshape, if not dominate, the international order. As the National Security Strategy of the United States[2] puts 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." For the IC, this rivalry will govern not only what U.S. leaders ask of it, but also how it must evolve. Despite the urgency of the threat, the preponderance of IC collection and analysis resources is still heavily focused on traditional national security threats rather than economic competitiveness issues. This balance needs to shift to

[1] The concept was first introduced in Anthony Vinci, The Coming Revolution in Intelligence Affairs, Foreign Affairs (2020).
[2] National Security Strategy, The White House at 23 (2022).

enable the IC to better protect U.S. supply chains and intellectual property and to slow down our adversaries' progress in some critical technologies such as AI.

- ***Produce net assessments on key technological trends.*** To better understand the techno-economic threat landscape, the next Director of National Intelligence (DNI) should task the National Intelligence Council (NIC) and the new Office of Economic Security & Emerging Technology (OESET) to prepare an analysis of what new and emerging technologies will matter for future U.S. competitiveness and national security. These organizations should orchestrate regular technology "net assessments" that compare U.S. and foreign capabilities to identify gaps and guide policy and resource decisions. These assessments should harness the insights and knowledge of the private sector, both domestic and in allied countries, and be briefed to Congress and the American people on an annual basis, alongside the Annual Threat Assessment.

- ***Establish new collection priorities.*** The NIC's analysis should then be used as a prioritization framework for intelligence collection, and the Central Intelligence Agency (CIA), National Security Agency (NSA), National Geospatial-Intelligence Agency (NGA), and the Department of Treasury should allocate, shift, and coordinate resources to better target foreign techno-economic issues, particularly on China. Techno-economic collection should rise in importance in the President's Intelligence Priorities list and the National Intelligence Priorities Framework, with some issues being designated as either Tier 1 or Tier 2 priorities.[3] This directive should emphasize collection priorities not only on the current technological state-of-play but also on future development and dual-use capabilities.

- ***Decisively enhance the agility and responsiveness of U.S. economic statecraft.*** The CIA, at the direction of the President, should identify opportunities and implement procedures to counter economic encroachments by the PRC and other adversaries, including supply chain disruptions, intellectual property theft, and predatory investing practices. As part of these efforts, the CIA should have expanded authorities to inform and advise U.S. companies about potential vulnerabilities and ways they can bolster their defenses against foreign intrusions and intellectual property theft. The intelligence components of the Federal Bureau of Investigation, the Department of Homeland Security, and the Department of Commerce should be given clear direction to devote more attention to protecting the nation's critical infrastructure and supply chains. Commerce, in particular, should augment its Office of Intelligence and require more of its Bureau of Industry and Security staff to hold security clearances so they can drive the intelligence requirements process.

Objective 2: Establish a new and fully funded institutional home for Open Source Intelligence.

Outside of the IC, private companies, researchers, and foreign competitors are taking full advantage of the explosion of publicly-available digital data to better understand the world, yet inside the IC so-called "Open Source Intelligence" (OSINT) remains under-resourced and under-utilized. To reverse this trend,

[3] Intelligence Community Directive 204, National Intelligence Priorities Framework, Office of the Director of National Intelligence (2021).

the CIA's Open Source Enterprise should be transferred to the Director of National Intelligence and renamed the National Open Source Center (NOSC), on par with the National Counterterrorism Center and National Counterintelligence and Security Center. Its director would report directly to the DNI, and the Center's staff should be increased by at least 100 employees. It would be OSC's mission to carry out the following:

- ***Organize the IC's collection of foreign media and other publicly available sources.*** OSC should lead in setting standards and guidelines that harmonize how the IC gathers, stores, and shares open source data across the National Security Enterprise (NSE) to enable maximal use of artificial intelligence and other big data techniques. OSC should also establish a new public-private partnership – the IC Data Consortium[4] – to ensure the U.S. Government has access to the very best commercially-available data sources at a reasonable cost. IC components seeking to acquire open source data should be required to do so via OSC to avoid duplication and to ensure the data is available across the IC via AI-enabled tools.

- ***Assume primary responsibility for day-to-day information collection on so-called "Global Coverage" topics for which there normally is very little intelligence information available.*** The United States has global interests and responsibilities, yet we cannot afford to have the IC's precious sensitive collection systems cover everything around the globe. For non-priority issues, such as political and economic trends in small nations, transnational migration flows, or climate change, OSINT entities can fill collection gaps at relatively low cost and risk, freeing up the rest of the IC enterprise to focus on hard targets.

In addition, the Intelligence Community should be more open to sharing high-quality analyses and assessments that are derived from unclassified sources by think tanks, commercial companies, and academic experts, particularly when they offer unique and timely insights outside of the IC's traditional areas of expertise. The IC should make more of an effort to make some of its analysis available at the unclassified level to better inform the public and help support U.S. strategic narratives.

- ***Direct the National Intelligence Council (NIC) to curate the best-in-breed open source assessments from the private sector, academia, and think tanks.*** While nothing can replace the value of the IC's all-source assessments on national security topics where there is a depth of exclusive intelligence reporting, the same cannot be said for many techno-economic issues that are vital to national competitiveness, but for which clandestine collection is lacking. On a growing range of issues – from PRC domestic microchip production, Russian efforts to evade financial sanctions, or terrorists' use of bitcoin[5] – commercial vendors, independent online investigators, and researchers are ahead of the IC in providing cutting-edge assessments on topics that matter for U.S. competitiveness. To address the shortfall, the NIC should be directed to build and maintain a library of high-quality unclassified analyses from vetted providers and make them

[4] See Intelligence Innovation: Repositioning for Future Technology Competition, Special Competitive Studies Project (2024) for additional detail on the proposed mission and structure of the new consortium.

[5] Dylan Patel, et al., China AI & Semiconductors Rise: US Sanctions Have Failed, SemiAnalysis (2023); Al Maggar, War Machine: The Networks Supplying & Sustaining the Russian Precision Machine Tool Arsenal, C4ADS (2024); Eitan Danon, Cryptocurrency in the War Zone: A Closer Look at Recent Events in Syria, ChainAnalysis (2024).

available to the President and U.S. officials via the President's Daily Brief and other channels as part of its all-source analytic service to policymakers.

- ***Expand the use of "strategic declassification" to support U.S. strategic messaging and educate the public about techno-economic threats.*** Used selectively and with precautions to protect fragile intelligence sources and methods, releasing declassified assessments on foreign threats can bolster domestic and international support for U.S. policy objectives. We urge the incoming administration to build on its track record of declassification decisions it made during the previous Trump administration[6] and engage the IC in using the declassification tool to expose foreign cyber and ransomware attacks, IP theft, and anti-competitive trade or financial practices.

Objective 3: Prioritize the formation of strategic intelligence alliances to dominate the techno-economic advantage.

In order to stay up to speed on the latest technological breakthroughs and position itself to take advantage of them to further U.S. national security interests, the IC needs a closer relationship with U.S. industry, U.S. academic experts, and select allied nations. Winning the technology competition for the IC also necessitates a new level of innovation and speed. To achieve that goal, IC agency leads should eliminate existing barriers that inhibit rapid onboarding of emerging technologies and reduce the IC's over-reliance on larger so-called "prime" contractors that are easier to work with but often offer little innovation.

- ***Create an IC Technology Advisory Council.*** The DNI, DCIA, and leaders from across IC elements should institute a Technology Advisory Council to inform interagency leaders on technology trends and emerging capabilities. The council should be composed of leading experts from industry and academia that meet on a regular basis determined by the interagency leadership and developments in technology trends.

- ***Forge tighter partnerships with the private sector.*** The IC should create the infrastructure and policies necessary to facilitate a broader exchange of information with the private sector. This will help enhance national competitiveness and resiliency against threats. As part of this effort, the IC should create a new National Intelligence Capital Office (NICO) to attract funding from the private sector for scaling technological solutions to intelligence challenges. The NICO would not focus on incubating new technologies – a task best left to IQT – but rather focus on assisting companies with proven technology solutions to bridge the so-called "valley of death" and reach market viability.

- ***Accelerate AI employment and efficiency.*** The biggest impediment to accelerated deployments within the IC is self-imposed red tape. Incoming senior IC leaders should insist on faster innovation and eliminate cumbersome approval processes. Senior leaders should also make full use of the Other Transactional Authority (OTA) Congress has granted them to speed up deployments of AI systems and set specific and ambitious goals for their expanded use. Building on the 2021 statements by the Senate Select Committee on Intelligence,[7] ODNI and IC leaders

[6] See e.g., Declassification Diplomacy: Trump Administration Turns Over Massive Collection of Intelligence Records on Human Rights and Argentina, The National Security Archive of The George Washington University (2019).
[7] Intelligence Authorization Act for Fiscal Year 2022, Senate Select Committee on Intelligence (2021).

are encouraged to "enter into grants, cooperative agreements, and other transactions" with non-governmental entities for R&D activities using existing authorities. The acquisition process should prioritize contracts and agreements with smaller firms to encourage innovation. The acquisition process should prioritize contracts and agreements with smaller firms to encourage innovation, building on an existing growth rate of 2.5 for federal spending on AI contacts, as seen from 2017-2022. Similarly, there should be a more concerted effort to allocate funds from existing budgets towards more R&D, an effort which already has the support of the Bipartisan Senate AI Working Group.[8]

Objective 4: Provide the President with the Means to Push Back Against Threats.

Incidents such as the "Salt Typhoon" hack of U.S. telecom companies by the PRC[9] show that our adversaries are increasingly able to penetrate our cyberspace with little cost or consequence. Russia and Iran are now even emboldened to undertake brazen assassination and sabotage plots overseas, including against the President-elect.[10] The IC needs to put itself more on a warfooting and be ready to respond quickly and effectively should the President direct it to defend the nation and prevent unacceptable behavior by the Axis of Disruptors. As Israel demonstrated so convincingly last year against Hezbollah, HAMAS, and Iran, the selective application of bold, creative, covert actions can have a decisive impact.[11] Whether the United States undertakes such actions must necessarily be a policy decision, but the IC has an essential role to play in identifying opportunities and developing implementable plans.

- ***Create a cyber countermeasures playbook.*** The IC should proactively prepare by regularly updating contingency plans to counteract malign cyber activities, not just by observing them. Led by the NSA and CIA, the IC should develop covert capabilities to exact a cost from foreign malign cyber and ransomware actors who are attacking U.S. citizens, government agencies, and our private sector on a daily basis. Possible courses of action could include targeted covert action – including the destruction of cyber infrastructure – enabling punitive economic sanctions or law enforcement actions, or strategic declassification to expose malign activities. These IC options would be most effective were they part of a broader suite of possible non-intelligence-related policy options for countering cyberthreats.

- ***Disrupt authoritarian information domains.*** Regimes in the Axis of Disruptors pursue relentless disinformation campaigns targeting the United States and the West even as they deceive their own populations as to their true nature and cover up the domestic costs for their aggressive policies. China's Great Firewall[12] is increasingly becoming a model for repressive regimes around the world seeking to cut off their populations from the free flow of information. The CIA and

[8] Nihal Krishan, Federal Gov Spending on AI Hit $3.3B in Fiscal 2022: Study, FedScoop (2023); Driving U.S. Innovation in Artificial Intelligence: A Roadmap for Artificial Intelligence Policy in the United States Senate, The Bipartisan Senate AI Working Group (2024).
[9] Richard Forno, What Exactly is Salt Typhoon?, Stanford University School of Law Center for Internet and Society (2024).
[10] Jeff Stein, U.S. Imposes Russia, Iran Sanctions Over Attempted Election Interference, Washington Post (2024); Robert Legare, Iranian Operative Charged in Pre-Election Scheme to Assassinate Trump, Other U.S. Targets, CBS News (2024).
[11] Mark Mazzetti, et al., Behind the Dismantling of Hezbollah: Decades of Israeli Intelligence, New York Times (2024); David Brennan, Pagers, Beds, and Phones: Latest Lebanon Attack in Israel's History of Bold Covert Ops, ABC News (2024).
[12] China's Great Firewall, Stanford University Department of Computer Science (last accessed 2024).

NSA should be directed to develop a comprehensive covert action strategy to disrupt the ability of autocratic regimes to control their own information environments.

- ***Target adversaries' AI and prevent them from targeting our own.*** Within a few years -- almost certainly within the timespan of this presidency -- artificial intelligence systems are likely to mature to the point that they will become essential tools for national security decision making. Developing and protecting U.S. national security AIs will be essential, as will developing the means to counter the national security AIs of our adversaries. The NSA's Cybersecurity Collaboration Center should place a priority on hardening the security of frontier U.S.-developed models against foreign interference and espionage. And the NSA and CIA should be directed to develop the means to covertly disrupt adversaries' national security-related AI systems.

Objective 5: Transform The Future IC Workforce.

To provide actionable intelligence on evolving threats, the IC workforce must be trained on how to effectively utilize AI technology and be deft enough to adapt to future innovations. The IC must overhaul its recruitment and retention strategy to be one that identifies, rewards, and cultivates technological talent so that it becomes an attractive employer that is competitive with private industry.

- ***Re-invent how the IC recruits tech talent.*** IC agencies' recruitment efforts right now are too weighted toward weeding out candidates via the security vetting process. This is fine for many job categories, but to upgrade its technical prowess, the IC should pivot and start more actively wooing engineers and those with AI skills. To attract the best and the brightest STEM students, the DNI should amend its Centers for Academic Excellence program to focus on the country's top universities for engineering, physics, and computer science, enticing the next generation technical leaders to spend a portion of their careers helping further national security. Applicants who fulfill the IC's tech requirements should receive priority security clearance processing to avoid unnecessary delays in the hiring process, which might incentivize potential recruits to leave the process. Finally, while the IC should do what it can to offer these candidates a competitive wage and make full use of IC hiring authorities to offer one-time bonuses and higher pay grades to individuals with STEM skills, the IC should make creative use of top-level STEM new hires and put them to work on the IC's toughest and most compelling challenges right away. And – as will inevitably be the case for many young engineers – when they leave the IC to pursue private sector opportunities, IC agencies should find creative ways to maintain relationships with them by extending their eligibility for a clearance status, inviting them to act as technical consultants, or offering to enter into Collaborative Research & Development Agreements if their future work is relevant and of value to the IC.

- ***Accelerate rotational and other broadening opportunities with private industry and AI labs.*** Since technological development is happening primarily outside of government, it is essential that intelligence officers get exposed to that development through one-to-two-year secondment and rotation opportunities. IC components should expand pilot efforts like the Intelligence Community Public-Private Talent Exchange (PPTE) and Public-Private Analytic

Exchange Program (AEP),[13] which are aimed at growing expertise and deepening technical acumen, and use them to jump start AI expertise building in the IC. These opportunities should be coupled with promotion opportunities and/or retention benefits as well as longer length continuing service agreements.

- ***Make it easier for private sector experts to support the IC.*** The fast-pace of technological developments and the changing nature of work make it more likely individuals with tech skills will work on a variety of issues with multiple employers over the course of their careers. Rather than putting all their energy into recruiting young people to commit themselves to a career, IC components should invite talented researchers with key skills to serve 2-5 year contract assignments. These researchers could then retain their clearances after they have served and be available to consult or advise the IC on an "as needed" basis.

Conclusion

The IC is one of the United States' most crucial pillars in its national security apparatus and, therefore, one of the country's key guides for a rapidly evolving and uncertain future. To best position policymakers for this future, the IC must adapt to the times and become an entity that is more agile, future-thinking, and technologically-savvy. To achieve this, it must be open to new approaches to collection and analysis, partnerships and sources of talent, and risk thresholds. However, the IC will always be limited in its capacity to act, especially when it comes to covert action, so the executive and legislative branches must work in tandem with the IC to empower it to act and serve the nation's best interests and priorities.

---

[13] Intelligence Community Public-Private Talent Exchange, Office of the Director of National Intelligence (last accessed 2025); Public-Private Analytic Exchange Program (AEP) Deliverables, U.S. Department of Homeland Security (last accessed 2025).