MITRE | Intelligence After Next

2025 PRESIDENTIAL TRANSITION SPECIAL EDITION

MEETING THE CHINA CHALLENGE: KEY FOCUS AREAS FOR THE INTELLIGENCE COMMUNITY

by Margaret Stromecki

As part of MITRE's support to the 2025 Presidential transition, we are highlighting key Intelligence After Next (IAN) papers published recently for the Office of the Director National Intelligence (ODNI) and leaders within Intelligence Community (IC). Key topic areas include surveillance, privacy, transparency, and accountability; foreign policy; counterterrorism and cybersecurity strategies; combatant command support; and the future of the IC workforce. IAN papers aligned to these topic areas address key policy, acquisition and warfighting concerns and are as relevant in 2025 as when first published.

A Complex Challenge

The People's Republic of China (PRC) poses a complex and dynamic challenge to the U.S. Intelligence Community (IC). Organized to contain and deter the former Soviet Union, the IC pivoted to a unipolar world in the 1990s and to a laser focus on the Global War on Terror following the attacks of 9/11. However, neither adversarial engagement effectively prepared the IC for the predominant challenge of the 21st century: a rising, assertive, and resource-rich PRC that is seeking to upend the U.S.-dominated global world order.

The priority assigned to the China challenge in the 2023 National Intelligence Strategy (NIS) is clear, as it is imbedded in the first NIS Goal: "Position the IC for Intensifying Strategic Competition." The strategy names the PRC as the key competitor, characterizing the country as "the only U.S. competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do so."[1]

The IC must be prepared to support decision makers and warfighters along the competition spectrum, from low-scale tension to conflict. Like the competition with the Soviet Union, full-scale war between the United States and the PRC risks a global conflict or a nuclear exchange.

Unlike the Soviet Union, however, the PRC is an integral element of the global economy, a point demanding a more nuanced approach. Containment must fall short of full de-coupling, and any conflict is best restricted to the economic, technological, and information sphere parts of the competition spectrum. As stated in the National Security Strategy of 2022, the United States must "compete responsibly with the PRC to defend our interests and build our vision for the future."[2]

The IC needs to move beyond the sphere of military threats to encompass new business areas like emerging technologies and supply chain risks. If the IC makes this transition skillfully, it could be a leading contributor to the effort to keep the competition with the prc outside the realm of military conflict.

The IC currently is not positioned optimally to tackle the full spectrum of competition with the PRC. The IC is oriented to collect, analyze, and act on security threats to our military assets, our borders, our partners, and our intelligence apparatus. It needs to broaden capabilities in key areas, such as economic intelligence, and re-orient its approach toward the whole of government, efforts that will increasingly push it toward the open-source world and greater transparency with other government international partners.

As Congressional Representative Adam Schiff notes in his 2020 article in *Foreign Affairs*, "we need to change how we view the threat from China. Beijing presents not only a military threat but also economic, technological, health, and counterintelligence threats."[3]

Key Focus Areas

In conducting literature reviews, discussions with experts inside and outside government, and an assessment of gap areas in current IC capabilities, we have identified five focus areas requiring urgent attention, resources, and top-level government leadership engagement (Table 1).

Table 1: Key Focus Areas for Strategic Competition

Focus Area	Key Components
Economic and Technological Conflict	• Technical capabilities • Emerging technologies • Intellectual property theft and technology transfer • Currency manipulation • Sanctions and countersanctions
Global Influence Projection	• Disinformation, misinformation, and malicious information • Belt and Road Initiative • Taiwan and South China Sea provocations • Military power projection
Foundational Knowledge	• Language capabilities • Leadership decision making • Cultural attributes • Perception management • Order of battle and military capabilities
Supply Chain Threats	• Critical minerals • Chinese state and private investment in United States • Hidden Chinese ownership • U.S. vulnerabilities • Critical technologies
Intelligence Advantage	• Surveillance capabilities • Information access and gaps • Counterintelligence • U.S. vulnerabilities • Intelligence diplomacy • Cyber threats

Economic and Technological Conflict

The competition with China in the economic and technological arenas poses risks to our national security, the health of our innovation sector, the well-being of our citizens, and our ability to forge alliances through economic cooperation. As the IC grapples with the China challenge, it must address these arenas—which rival those of military threats. Indeed, the U.S. national security enterprise and the IC must incorporate economic and technological competition into their threat calculus.

- Countering China's economic espionage and its campaign of IP theft and technology transfers requires new skill sets in the IC's operational, analytic, and counterintelligence communities. Domestic agencies need staff who understand the signs of economic espionage and can gain access to those targets. Agencies focused on overseas efforts need to hone their capabilities in identifying, collecting information on, and analyzing technological targets in addition to traditional military and leadership targets.
- As military targets become increasingly software and artificial intelligence (AI) driven, it is incumbent on the IC to understand those complex technological systems. In their article "US-China Competition and Military AI: How Washington Can Manage Strategic Risks amid Rivalry with Beijing," Jacob Stokes and Alexander Sullivan key in on the Chinese military's use of AI and the need to prioritize collection and analysis in that area.[4]

The world's integrated global economy—dominated by the United States and the PRC—demands an understanding of the interplay among the actors and the implications of courses of action by policymakers. Because Chinese decision making is opaque, the IC can help fill gaps through enhanced economic analysis, the use of open-source data and advanced analytics, and modeling economic behavior.

- The IC can employ modeling techniques to predict likely courses of action by the PRC in response to U.S. initiatives like applying sanctions, protesting currency manipulation, or instituting further export controls. Involving experts outside the Community in developing scenarios, disruptive injects, and expected PRC norms and behaviors can enrich the sophistication of the models. Not only can these exercises illuminate possible actions, they also can develop the expectations of the outcomes of U.S. efforts and the utility of specific courses of action.

Countering China's economic espionage and its campaign of IP theft and technology transfers requires new skill sets in the IC's operational, analytic, and counterintelligence communities.

Global Influence Projection

China's efforts to increase its global influence run the gamut of building military bases, gaining economic dependence from states through the Belt and Road Initiative—the PRC's provision of loans and capabilities for infrastructure development—and using propaganda and disinformation to shape its image. While the IC naturally focuses on China's aggressive behavior in the Taiwan Strait and South China Sea to prepare the Department of Defense for possible armed conflict, agencies should also expand efforts to counter China globally to preserve the current global world order. Influence once gained is difficult to dislodge, and most nations are concerned with their own interests and are not focused on the U.S.-China competition.

The IC can support decision makers by methodically tracking Chinese global influence campaigns. Collectors and analysts should employ the diverse open-source data sets available to determine where the Chinese are investing, how receptive foreign governments and populations are to Chinese efforts, and what kinds of disinformation can be ascribed to the Bejing. Knowing Chinese power projection goals and where our global relationships are at risk will be critical for countering such campaigns.

- Modeling and simulation can illuminate investment patterns and help clarify for decision makers Chinese intentions for accruing influence through lending efforts and large infrastructure projects that create dependencies on the part of the host government and regional toeholds for the Chinese.
- AI capabilities including large language models can help determine the provenance of propaganda and disinformation and how those messaging campaigns are being received by host countries.

As China continues to build capacity in the South China Sea and the Global South, the IC can use analytic tools to support U.S. Indo-Pacific Command's efforts to strengthen U.S. power projection capabilities and the capacity of its allies to withstand a Chinese military assault on Taiwan or other U.S. partners. The fluid environment lends itself to knowledge graphs and dashboards that capture real-time inputs from both publicly available data and classified sources.

Foundational Knowledge

The IC suffers from a dearth of expertise and language capability on the China target. Some of this stems from counterintelligence concerns, and some stems from a lag in educational programs focused on China. During the Cold War, legions of IC collectors and analysts were trained in an array of Soviet studies programs, had extensive language capabilities, and had lived or studied in the USSR. Although this did not ensure that the IC had a complete understanding of Soviet thinking, the level of expertise brought the Community to a more sophisticated knowledge of the Russian mindset than it currently enjoys regarding PRC leadership thinking.[5]

- The IC must be resourceful in finding ways to partner with thinktanks, academics, and non-governmental organizations (NGOs) to amplify its own limited stable of Chinese experts. The large amount of data available in the open-source ecosystem will enable the IC to build robust relationships where collaboration can occur in an unclassified environment.
- Advanced analytic techniques like perception modeling and AI tools can enable translations on an enterprise scale can also help fill gaps in language and regional expertise.

The IC must also press forward with hiring talent with deep China expertise and training its current cadre of analysts and operators. Educational and thinktank programs focused on China are now flourishing in the United States, but it will take time to build a deep bench of experts.

- IC recruiters should engage energetically with China studies programs, as they once did with Soviet studies programs. Internally, the IC should fund current staff for educational programs, language training, and rotations to thinktanks focused on China to increase capabilities.

Supply Chain Threats

The interdependence reflected in the global economy presents an almost overwhelming array of supply chain risks. Our national security enterprise is as vulnerable as the private sector, and the IC needs to build capacity in understanding supply chains and identifying nodes of risk. The recent concern over the supply of semiconductors exposed just one example of the extent to which the United States and its national security infrastructure ely on products that would be in jeopardy during heightened conflict with China, even one that did not erupt into military combat.

- Reuters reported in December 2021 that 90 percent of high-end semiconductors are produced in Taiwan, a source that would be at critical risk during a conflict over the island.[6]

It is incumbent on the IC to develop models, recruit experts, and acquire data sets that can be analyzed to reveal supply chain components. The vast network of suppliers for the DoD and its reliance on critical minerals and exquisite technologies demand improved capabilities in the IC. The IC can exploit and learn from the techniques and skills developed to expose terrorist financing networks, and it will need to further

hone that craft to tackle the larger problem of hidden Chinese ownership of key industries and where U.S. vulnerabilities are most acute.

- According to a study from the Center for Strategic and International Studies, "DoD relies on contracts with prime contractors and expects those primes to manage their own supply chains, but too often that has proven to be a misplaced trust. … Companies may not know when an adversary or competitor acquires a sub-contractor, or the chain of custody or a critical widget might be obscured."[7]

Intelligence Advantage

The IC is facing a formidable challenge in the form of Chinese intelligence collection operations and must find a way to secure the advantage in the intelligence domain. According to the U.S.-China Economic and Security Review Commission's Annual Report in 2019, reports of Chinese espionage have risen significantly in recent years, and the level of intelligence activity has only increased since then. The most serious threats are the PRC's cyber, technical collection, and human penetration capabilities, both inside the United States and globally.[8] More recently, the Director of British Security Service (MI5) said Chinese espionage in the United Kingdom is on an "epic" scale, with Chinese spies attempting to make contact with more than 20,000 people.[9]

Given their large global footprint, Chinese intelligence services pose a threat to the IC around the world. Their surveillance capabilities—honed by their use domestically against their own citizens—and their commitment to projecting those capabilities pose broad risks. Collectors in the IC need to mitigate the risks posed by these expanding Chinese cyber and surveillance capabilities and modify their behaviors as required, a difficult, time-consuming, and resource-heavy requirement.

- Director of National Intelligence Avril Haines noted in her 2023 Annual Threat Assessment that China is probably the greatest cyber espionage threat to the U.S. government. The report states that "China's cyber espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations."[10]

An area to which the IC can contribute to the broader competition with China is intelligence diplomacy, a tool used with great effect to discredit Russia's efforts to distort messaging on its invasion of Ukraine in 2022. According to Assistant Secretary of the Bureau of Intelligence and Research at the State Department, "When we talk about intelligence diplomacy at the State Department, we mean that intelligence can serve as a key tool to inform, drive convergence in approaches and outlooks, enable common actions, and deprive adversaries of advantage."[11] Merging the IC's work with domains in other parts of the Interagency helps address the comprehensive, holistic challenge the PRC presents.

The Way Forward

The IC has the leadership and stellar track record to rise and meet this evolving challenge. We make the following recommendations to enable an effective transition:

Increase the capability to acquire and exploit open-source materials. As the competition with China moves beyond the military sphere, vast amounts of information are available publicly. The IC must improve its ability to acquire that data, structure it, integrate it with classified data, and exploit it with sophisticated tools. In his article for *Foreign Affairs*, Schiff advises that "Intelligence agencies must do a better job of adapting to the sheer amount of open-source data available to them about global threats and competitors and to quickly get the resulting intelligence to decision-makers."[12]

- As noted in previous MITRE publications, "Incorporation of commercially and publicly available data is only partly a technological challenge. It is also a governance challenge: that

of how to establish and maintain a regulatory, legal, and policy framework that permits effective data usage and sharing in support of a whole-of-nation strategy, but within the constraints consistent with American values."[13]

- Technologies such as large language models and other AI tools can help manage the increasing amounts of data. The IC must pivot toward exploitation that does not rely solely on human effort if it is to meet the challenge of information overload.
- Integration of diverse data sets within agencies and across the IC will be critical to surfacing key insights. Analytic tools that can be applied to multiple streams of data will prove far more effective for discovery than the often-used bespoke tools applied to single data sets.

Think Whole of Government. The IC must pursue the PRC threat with a focus on new partnerships within the government. Civilian entities like the Department of Commerce can provide information, expertise, and capabilities that the IC needs. Expanding interagency fora will offer opportunities to combine authorities for greater effect. The IC must also lean forward in sharing information with other agencies, a cultural shift that will require strong leadership to implement.

- The IC is tackling other challenges, like climate change, by bringing together working groups that include agencies like the National Oceanic and Atmospheric Administration (NOAA) and the national laboratories to broaden its impact. Using the National Security Council construct is a start, but the IC must proliferate working groups and senior leader engagements that include non-traditional partners that may not have access to classified information.

Engage outside experts. To compensate for a shortfall in internal expertise, the IC should expand on existing relationships with thinktanks, academics, and other experts and build new collaborations with a range of outside voices. Greater use of open-source materials will enable fruitful exchanges and build capacity in new business areas for the IC.

- The Washington, D.C. area is home to a host of non-partisan thinktanks and academic institutions that have access to experts with experience in the PRC. These resources can serve as a force multiplier for the IC's relatively small cadre of deep experts and provide critical understanding of the cultural forces shaping Chinese leadership behavior.

Invest in translation tools. IC agencies should collaborate in adopting translation tools that are scalable and capable of translating complex information sources like PDFs, handwritten Mandarin characters, and highly technical reports. Absent these translation capabilities, the IC will miss out on critical data that decision makers need.

- The commercial sector continues to improve its ability to translate Mandarin Chinese, and the IC needs to partner with those companies that are demonstrating their capability. The IC should take cues from those agencies that have effectively partnered with the private sector to incorporate commercial solutions into their workflows. The Office of the Director of National Intelligence (ODNI) could provide leadership through funding and mechanisms like the Intelligence Advanced Research Projects Activity (IARPA) to convene the Community and push forward IC-wide capabilities.

Expand collection and analysis in new areas. The IC should build collection, analysis, and expertise in new areas of concern like supply chains, PRC emerging technologies, intellectual property theft, and Committee on Foreign Investment in the U.S. issues. Addressing the totality of the competition spectrum requires an expansion of focus.

- Agencies should articulate information needs and identify gaps in collection in new business areas. Requirements might be met by acquiring commercial data sets, exploiting publicly available information like Chinese scientists' research

papers, or identifying innovative methods for collecting information. In parallel, the IC must hire or train experts who understand emerging disruptive technologies and can assess the implications for Chinese innovation.

The Time Is Now

The IC can and must pivot to meet this new challenge. The tragedy of 9/11 pushed the IC toward greater collaboration and information-sharing through new institutions like the ODNI and entities like the National Counter-Terrorism Center, with its focus on data fusion. The competition with the PRC must deliver a similar transformation in the way the IC does business.

The days of relying exclusively on exquisite collection to produce relevant insights for decision makers are over. The wealth of open-source data available should push the IC to apply resources to data integration, fusion, and analysis with the same commitment it has dedicated to clandestine collection. That shift will require a change in culture driven by IC leaders' resourcing decisions and mission priorities.

The IC needs to move beyond the sphere of military threats to encompass new business areas like emerging technologies and supply chain risks. Much of the IC—particularly military-civilian hybrid agencies like the National Security Agency and the Defense Intelligence Agency—focuses on warfighter support and tactical intelligence. The new paradigm encompasses a much broader scope of competition and should expand beyond combat readiness.

The IC has proved itself agile and responsive throughout its history, particularly when faced with a national-level crisis. If the IC makes this transition skillfully, its agencies could be a leading contributor to the effort to keep the competition with the PRC outside the realm of military conflict.

References

1. Office of the Director of National Intelligence, National Intelligence Strategy, 2023. Available: https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2023.pdf
2. The White House, National Security Strategy, October 2022. Available: https://www.whitehouse.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf
3. Adam Schiff, The US Intelligence Community Is Not Prepared for the China Threat, Foreign Affairs, September 2020. Available: https://www.foreignaffairs.com/articles/united-states/2020-09-30/us-intelligence-community-not-prepared-china-threat
4. Jacob Stokes and Alexander Sullivan with Noah Greene, US-China Competition and Military AI: How Washington Can Manage Strategic Risks amid Rivalry with Beijing, Center for a New American Security, July 2023. Available: https://www.cnas.org/publications/reports/u-s-china-competition-and-military-ai
5. Adam Schiff, The US Intelligence Community Is Not Prepared for the China Threat, Foreign Affairs, September 2020. Available: https://www.foreignaffairs.com/articles/united-states/2020-09-30/us-intelligence-community-not-prepared-china-threat
6. Yimou Lee, Norihiko Shirouzu, and David Lague, Taiwan Chip Industry Emerges as Battlefront in US-China Showdown, Reuters, December 2021. Available: https://www.reuters.com/investigates/special-report/taiwan-china-chips/
7. Emily Harding and Harshana Ghoorhoo, Building Supply Chain Resilience, Center for Strategic and International Studies, December 2022. Available: https://www.csis.org/analysis/building-supply-chain-resilience
8. The U.S.-China Economic and Security Review Commission, Annual Report to Congress, November 2019. Available: https://www.uscc.gov/sites/default/files/2019-11/2019%20Annual%20Report%20to%20Congress.pdf
9. Maroosha Muzzaffar, MI5 Boss Says Chinese Espionage in UK on 'Epic' Scale with 20,000 People Approached by Spies, Independent, October 18, 2023, https://www.independent.co.uk/news/uk/home-news/ken-mccallum-mi5-boss-chinese-espionage-uk-b2431541.html
10. Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community, February 2023. Available: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf
11. Assistant Secretary Brett Holmgren, Bureau of Intelligence and Research, Department of State, Intelligence and Diplomacy: A New Model for a New Era, Cipher Brief Annual Threat Conference remarks, October 2023. Available: https://www.state.gov/intelligence-and-diplomacy-a-new-model-for-a-new-era/
12. Adam Schiff, The US Intelligence Community Is Not Prepared for the China Threat, Foreign Affairs, September 2020. Available: https://www.foreignaffairs.com/articles/united-states/2020-09-30/us-intelligence-community-not-prepared-china-threat
13. MITRE Center for Strategic Competition, Using Publicly Available Information in American "Whole-of-Nation" Strategic Competition, November 2022. Available: https://www.mitre.org/news-insights/publication/public-information-american-whole-of-nation-strategic-competition

Author

Margaret Stromecki, a systems engineering principal, leads the Counter-PRC Cell in MITRE's National Security Sector (MNS). In this position, she manages internal projects related to the challenges posed by the strategic competition with the PRC; serves as a focal point for MNS on issues related to the PRC; and conducts outreach to sponsors working in the PRC mission space. Margaret joined MITRE following a career at the Central Intelligence Agency, where she was a senior executive in the Directorate of Analysis. She has a B.A. in Government and Soviet Studies from Cornell University and an M.A. in International Affairs from Columbia University.

Intelligence After Next

MITRE strives to stimulate thought, dialogue, and action for national security leaders developing the plans, policy, and programs to guide the nation. This series of original papers is focused on the issues, policies, capabilities, and concerns of the Intelligence Community as it prepares for the future. Our intent is to share our unique insights and perspectives surrounding a significant national security concern, a persistent or emerging threat, or to detail the integrated solutions and enabling technologies needed to ensure the success of the Intelligence Community. The views expressed in this publication are those of the author(s) and do not imply endorsement by the Office of the Director of National Intelligence or any other U.S. government department/agency.

You can receive all of MITRE's Intelligence After Next papers by subscribing to the series at mitre.org/IntelligenceAfterNext

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded research and development centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.