Statement before the House Permanent Select Committee on Intelligence

"2024 Priorities for the Intelligence Community and Intelligence Committee in the Face of Worldwide Threats"

A Statement by:

Kari A. Bingen

Director, Aerospace Security Project, and Senior Fellow, International Security Program, CSIS

May 15, 2024

HVC-210

Chairman Turner, Ranking Member Himes, and distinguished Members of the Subcommittee, thank you for the invitation to appear before you today. It has been a privilege working with this Committee and supporting many of you while a staffer on the Armed Services Committee. I am grateful for this Committee's steadfast support of the Intelligence Community (IC) and especially of the defense intelligence enterprise, which I was honored to help lead while serving as Deputy Under Secretary of Defense for Intelligence and Security. My admiration for our intelligence professionals only grew while I served in the Department of Defense (DoD) and saw firsthand their dedication to mission and to our national security.

I cannot overemphasize how acute the security challenges are before us, the technology trends occurring around us, and the significant changes underway to posture the intelligence community (IC) for the competitive and contested environment we face. Adversary threats are increasing in speed, scale, and complexity, and are made even more difficult by the increasing collaboration across threat actors and simultaneity of crises and challenges upon us. We will have to question our assumptions, our policies and processes, and our ways of conducting intelligence activities that have been enshrined in our thinking over the last several decades.

Today, for your consideration, I offer observations on five aspects of the intelligence enterprise that are vitally important for the United States' maintaining an advantage in this competitive and contested security environment. I make these observations largely through a defense intelligence lens, knowing that my colleagues on this panel complement my knowledge across other areas of the IC and its missions.

Reclaiming our ISR Advantage

First, our intelligence, surveillance, and reconnaissance (ISR) capabilities are under increasing threat while our adversaries' ISR is rapidly advancing. Many of our ISR systems and operating concepts assume air, space, and spectrum superiority. We built large, exquisite satellite systems and controlled overseas drones from ground stations in the United States using satellite communications (SATCOM) and Global Positioning System (GPS) navigation. However, against a sophisticated adversary with anti-satellite weapons, robust air defenses, and ways to jam SATCOM and GPS, these ISR systems and operating models will be increasingly under strain. Such operational threats are driving investments towards more resilient architectures, including proliferated ISR satellite constellations, and networking solutions that create multiple pathways to deliver intelligence data to users.

Meanwhile, foreign advances in ISR, including ubiquitous sensing and artificial intelligence (AI), will make it more difficult for our military forces and intelligence operatives to maneuver undetected. Surveillance cities, sophisticated digital monitoring, and advanced analytic tools employed by our adversaries will make other aspects of intelligence, such as human intelligence (HUMINT) operations and the use of cover, increasingly harder. Such constant surveillance –

whether through space, terrestrially, or in cyberspace – will necessitate new or modified capabilities, tactics, training, and tradecraft.

In space, the majority of recently launched Chinese satellites have been ISR satellites, which extend Beijing's surveillance into space. According to U.S. Space Command, as of January 2024, China had approximately 360 ISR satellites on orbit, more than triple the number in 2018.[1] In August 2023, Beijing launched the world's first geosynchronous orbit (GEO)-based synthetic-aperture radar (SAR) satellite and in December 2023, it launched an optical imagery satellite to GEO, Yaogan-41. When paired with data from other Chinese ISR satellites, AI to rapidly identify objects, and networked communications systems, the People's Liberation Army (PLA) is quickly closing its own sensor-to-shooter kill chains across the Indo-Pacific.[2] Our military forces will need to train under the assumption that they will be seen, located, and targeted.

Revitalizing Foundational Military Intelligence and Scientific and Technical Intelligence

Second, our peer adversaries are developing more technically advanced and complex military systems that we need to understand to defeat. This will place increasing demands on our foundational military intelligence (FMI) and scientific and technical intelligence (S&TI) capabilities, which received less emphasis over the last 20 years. During this time, China and Russia made substantial progress in developing and fielding hypersonic missiles, anti-satellite weapons, electronic warfare and cyber-attack weapons, and undersea systems, to name a few.

FMI involves developing a comprehensive understanding of foreign militaries, including their facilities, organizational units, and capabilities.[3] S&TI involves the in-depth technical analysis of foreign weapon systems, including performance, vulnerabilities, how they're networked and controlled, and how they're integrated into broader military operations. This analytic knowledge informs our development of defenses and countermeasures, as well as ways to defeat these systems. S&TI centers, such as the National Space Intelligence Center (NSIC), National Ground

[1] Gregory Gagnon, "Implementing Competitive Endurance: Space Intelligence," transcript of speech delivered at the Center for Strategic and International Studies, October 10, 2023, https://www.csis.org/events/implementing-competitive-endurance-space-intelligence; Clayton Swope, Kari Bingen, Makena Young, Madeleine Chang, Stephanie Songer, and Jeremy Tammelleo, *Space Threat Assessment 2024* (Washington, D.C.: Center for Strategic and International Studies, 2024), 9, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-04/240417_Swope_Space_Threat_0.pdf?VersionId=DDeJ0EkYnF5W7POfMJHVGjkxEVeTx3o0.

[2] Clayton Swope, Kari Bingen, Makena Young, Madeleine Chang, Stephanie Songer, and Jeremy Tammelleo, *Space Threat Assessment 2024* (Washington, D.C.: Center for Strategic and International Studies, 2024), 9, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-04/240417_Swope_Space_Threat_0.pdf?VersionId=DDeJ0EkYnF5W7POfMJHVGjkxEVeTx3o0; Clayton Swope, "No Place to Hide: A Look into China's Geosynchronous Surveillance Capabilities," Center for Strategic and International Studies, January 19, 2024, https://www.csis.org/analysis/no-place-hide-look-chinas-geosynchronous-surveillance-capabilities.

[3] Scott D. Berrier, "Billington Cybersecurity Summit Fireside Chat with DIA Director LTG Scott D. Berrier," by David Frederick, Defense Intelligence Agency, September 9, 2022, https://www.dia.mil/Articles/Speeches-and-Testimonies/Article/3154271/billington-cybersecurity-summit-fireside-chat-with-dia-director-ltg-scott-d-ber/.

Intelligence Center (NGIC), and the Office of Naval Intelligence (ONI), provide such detailed analysis of foreign weapons, air, space, and undersea systems.

I would also call your attention to the Defense Intelligence Agency's (DIA) Machine-assisted Analytic Rapid-repository System (MARS) program – an effort to modernize our master data repository of FMI information. This is critical as today's platform rests on 1980s database technology and is severely limited in capturing richer data sources, more dynamic targets, and newer military activities, including in space and cyberspace, necessary to support intelligence analyses, military operations, and activities with allies and partners.[4]

Harnessing Technological Change from Outside Government

Third, while the IC maintains exquisite intelligence capabilities and proficiencies, I would observe that many of the most consequential technological advancements are occurring in the private sector and are being fueled by private capital. These advancements have the potential to revolutionize how the IC collects and analyzes information, but they will challenge culture and existing ways of doing business.

Generative AI and advanced compute are prime examples of this. Based on research by Goldman-Sachs, global AI investments are estimated to approach $200 billion by 2025,[5] in contrast to U.S. government investment at less than $5 billion.[6] The IC cannot replicate private sector AI and compute in scale, speed, or investment. For the IC to take full advantage of large-scale compute and generative AI – wherein machines can contextually learn, synthesize, and generate data across images, signals, and text – it will need to figure out how to work across both large-scale unclassified and classified compute environments.

While at the Pentagon, I recall pressing my daily intelligence briefer to provide deeper insights and context on topics than what I could access via open source. The advances described above can aid analysts in identifying patterns, drawing out unique connections across classified and unclassified datasets, and making sense of vast amounts of data that humans can't process at scale. But we will also need to think through how to harmonize analytic tradecraft and human expertise with machine-generated analysis.

This technology can be harnessed for good, but can also lead us astray. Generative AI can create new kinds of deception, obfuscation, and disinformation at machine speeds. The IC must have an

[4] Defense Intelligence Agency, "Machine-assisted Analytic Rapid-repository System (MARS)" (slides, Armed Forces Communications and Electronics Association Luncheon, June 21, 2019).
[5] Goldman Sachs, "AI investment forecast to approach $200 billion globally by 2025," August 1, 2023, https://www.goldmansachs.com/intelligence/pages/ai-investment-forecast-to-approach-200-billion-globally-by-2025.html.
[6] Jacob Larson, James S. Denford, Gregory S. Dawson, and Kevin C. Desouza, "The evolution of artificial intelligence (AI) spending by the U.S. government," Brookings Institution, March 26, 2024, https://www.brookings.edu/articles/the-evolution-of-artificial-intelligence-ai-spending-by-the-u-s-government/.

in-depth understanding of these technologies in order to develop ways to mitigate such threats. We will need to expand traditional analytic disciplines like foreign denial and deception to account for these technology trends.

There is also a growing tension between the speed and depth of analysis: getting tactical ISR data directly and quickly to warfighters versus providing analysis, context, and verification of information. While this should not be an either-or choice, technological advancements in automation and AI are making possible different constructs for user access to data and information. Particularly in the space arena, private companies operating satellite constellations in the hundreds to thousands are leveraging automation, advanced processing, and AI to optimize their operations and quickly draw insights from collected data. These advancements present opportunities for the IC to think differently about its satellite tasking and dissemination models, allowing for more direct tasking by users, direct downlink of satellite data to tactical nodes, and greater AI-enabled analysis.

A common theme here is that much of these technological advancements are occurring in the private sector, outside of the U.S. Government and outside the United States. We are in a technology race with China, which is after the same advanced technology that we are – AI, aerospace, quantum, microelectronics, biotechnology, etc. – for both military and economic benefit.[7] Many of the trends and insights about this techno-economic competition will not be found in highly classified reporting, but rather in understanding the flow of private capital, global supply chains, academic research, and business dynamics. Much of this can be gained through greater interaction with the private sector that competes with Chinese entities globally and on a daily basis. There is a need for intelligence analysts to understand this aspect of the global landscape and how U.S. competitiveness affects national security.

Securing our People, Information, and Business Advantage

Fourth, please continue to pay close attention to the security and counterintelligence mission of the IC, including industrial security and personnel vetting. While not a high-profile IC mission or program, security and counterintelligence underpin all activities that the IC and DoD undertake. You know this well, but it bears emphasis: Beijing continues to comprehensively target U.S. technologies, intellectual property, supply chains, and critical infrastructure across government, industry, and academia. It is playing the long game to penetrate our technology base and steal our information, using both legal and illegal means, such as foreign capital, economic espionage, cyber data exfiltration, and talent recruitment programs.[8]

[7] Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community" (Washington, DC: U.S. Government, 2024), 7-13, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.

[8] National Counterintelligence and Security Center, Office of the Director of National Intelligence, *Foreign Economic Espionage in Cyberspace* (Washington, DC: U.S. Government, 2018), 5-7, https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

Much of the contact layer being targeted by our adversaries is outside government, in the private sector and academia. This necessitates the importance of education and engagement, as well as greater transparency on foreign threats and tactics, and communicating these in ways that resonate with and move at the speed of business. The National Counterintelligence and Security Center (NCSC) and Defense Counterintelligence and Security Agency (DCSA) are progressing in the right direction: from "checklist-based" approaches to industrial security towards more threat-informed, risk-based approaches to assess and mitigate vulnerabilities.

I would also encourage strong oversight of the government's efforts to reform personnel vetting, including improving the clearance review and adjudication process. Continuous evaluation is an important step forward, but continue to push on personnel vetting reforms, reciprocity, and IT system modernization. With access to myriad data sources and advances in data analytics, there are smarter ways to assess and monitor personnel risks than current methods. The IC will simply not be competitive in attracting top, diverse talent if candidates are waiting months or years for a security clearance.

Developing our Workforce

Finally, I would recommend a comprehensive examination of workforce development within the IC. Candidly, this is an area in which I wish I had paid more attention. A big idea for the Committee's consideration is whether personnel reforms analogous to those in the Goldwater-Nichols Act of 1986 are needed to guide how the IC manages the career paths and professional development of its workforce. Goldwater-Nichols was a catalyst for enhancing operational effectiveness, building a joint force, and developing more well-rounded military leaders through professional military education and joint assignments that broaden their perspectives and cross-service relationships.

While the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 sought some changes similar to Goldwater-Nichols, it did not go far enough and implementation has been mixed. My observation is that the IC could be stronger in how it cultivates its workforce, especially for those seeking promotions into leadership roles. Such career enhancing and stimulating experiences are also important to nurture and retain talent, build collaborative relationships across the IC, and enhance mission effectiveness.

In full disclosure in my role as a member of the National Intelligence University's Board of Visitors, I see greater opportunity for professional education, akin to joint professional military education (JPME). I also see a need to broaden the knowledge and experience base for intelligence professionals – whether in conducting strategic research and analysis outside their day-to-day workflows, understanding their portfolio from different organizational perspectives, or experiencing firsthand the technology, capital, and global competitive dynamics at play through a public-private sector talent exchange. While largely anecdotal, I observed numerous joint duty

assignment (JDA) professionals return to home organizations only to be relegated back to similar positions that they had left.

Conclusion

Throughout the Cold War, the United States competed politically and militarily, but never economically, with the Soviet Union. For the first time, our nation faces a strategic competitor with the resources and potential to match, if not one day exceed, the size and scope of U.S. economic might and to develop new technologies that rival our own. Over the last 40 years, the United States has had to adapt several times to a new geopolitical and strategic environment, first after the collapse of the Soviet Union and then, after the September 11 attacks.

Now 20 years after the IRTPA and the establishment of the Director of National Intelligence, we face yet another new and evolving global landscape. We are still learning how to adapt our intelligence and defense mindsets, processes, and systems to this new environment in which we face an adversary with economic and military potential unlike anything we've faced in the past. We have a window to get this right and are fully capable of rising to the challenge.