STATEMENT OF

MS. ASHLEY MANNING

PERFORMING THE DUTIES OF ASSISTANT SECRETARY OF DEFENSE FOR CYBER POLICY

TESTIMONY BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON CYBERSECURITY, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

APRIL 10, 2024

Introduction

Chairman Gallagher, Ranking Member Khanna, and distinguished members of the Committee, thank you for inviting me to testify on the Department of Defense's cyber posture and the advancements we continue to make operationalizing the Department's priorities in cyberspace. It is an honor to appear alongside General Haugh, the Commander of U.S. Cyber Command (USCYBERCOM), who brings a breadth of experience to this position as we strive to keep pace with the rapidly evolving threat environment in cyberspace.

In my role Performing the Duties of Assistant Secretary of Defense for Cyber Policy, I am committed to providing overall supervision of the Department's policy for cyber, advancing the Department's strategic approach to cyberspace, and ensuring our readiness to counter emerging cyber threats. Mr. Chairman, I look forward to working with this Committee through my newly established office to further these objectives.

I come to this role as a career civilian with almost twenty years of service in the Department of Defense. I have had the privilege of working across a wide range of regional and functional issues including serving as Acting Deputy Assistant Secretary of Defense for the Middle East and the Principal Director for Plans and Posture in the Office of the Under Secretary of Defense for Policy. I also served as an exchange officer at the UK Ministry of Defence, where I was the Deputy Head of Strategy and oversaw the development of Defence's contribution to the UK Integrated Review strategy. In each of these roles, I have witnessed the cross-cutting role cyber plays in the defense of our Nation and our Allies and partners.

The President has nominated Dr. Michael Sulmeyer as the ASD for Cyber Policy. Should he be confirmed, I look forward to serving as the Principal Deputy Assistant Secretary of Defense (PDASD) for Cyber Policy.

Security Environment

Cyberspace serves as a cornerstone of global connectivity, communication, and innovation. It has revolutionized industries, bolstered our national prosperity, and enhanced the agility of our Joint Force. However, it also exposes us to diverse threats from malicious cyber actors seeking to exploit this interconnectedness for their own gain. Defending against these threats, both domestically and abroad, is paramount for the Department of Defense.

The People's Republic of China

Our National Defense Strategy (NDS) makes clear that the People's Republic of China (PRC) remains an enduring cyber threat and the Department's pacing challenge in cyberspace, as the PRC continues to target U.S. networks in prolonged campaigns of espionage and to pre-position its cyber forces for future operations. The PRC views cyber and information dominance as critical advantages, spurring continued investment in the technology sector and cyber forces. A key component of the PRC's strategy includes substantial investment in cyber espionage efforts, such as stealing intellectual property, research, and sensitive information from American citizens. This steady drain of sensitive U.S. information over time has the potential to erode advancements in U.S. military capabilities and the Joint Force's ability to project power.

In addition, a group of PRC cyber actors known as "Volt Typhoon" were first observed in mid-2023 pre-positioned on multiple critical infrastructure networks for potential disruptive or destructive cyberspace attacks in the event of a major crisis with the United States. These cyber threat actors leverage a technique referred to as "living off the land," which allows them to blend in with normal system and network activities, evading detection and making it very difficult to identify "Volt Typhoon" actors. These potentially destructive operations are part of a broader cyber campaign driven by PRC national and military objectives, one the Department is prepared to meet to preserve the ability of the Joint Force to fight and prevail in a contested cyberspace environment.

The PRC views information as a tool to be tightly controlled in service of consolidated authority. This is evident in PRC vulnerability disclosure regulations that mandate companies to report software vulnerabilities to government authorities within forty-eight hours of discovery, expanding the government's mass collection of software vulnerabilities. These requirements continue to exacerbate the challenge PRC cyberespionage and pre-positioning poses to the United States and our partners, because they provide PRC offensive cyber forces a virtual warehouse of cyber weapons that can be leveraged with impunity by the PRC government. Due to the dynamic nature of the cyberspace operating environment and the constant discovery and patching of software vulnerabilities, maintaining a new and robust list of vulnerabilities provides a distinct advantage.

Russia

Russia remains an acute threat to the United States and our Allies and partners as it continues to leverage cyberspace to target critical infrastructure networks and enable its malign influence operations. Russia maintains concurrent cyber campaigns targeting potential victims in the United States and North Atlantic Treaty Organization (NATO) nations and considers maintaining an ability to disrupt and degrade critical infrastructure Industrial Control Systems as a priority. Russia continues waging its war on the people of Ukraine, including by employing a range of cyber capabilities to disrupt Ukrainian military operations and erode political will for Ukraine's defense. Last year, Russian-linked cyber actors were observed spying on Android devices used by the Ukrainian military, providing an advantage to Russian military forces responding to Ukrainian military maneuvers. This past December, Ukraine was also the victim of a malicious cyber activity against its largest telecommunications provider, impacting millions of civilian subscribers in Ukraine. The ongoing unprovoked further invasion of Ukraine serves as a stark reminder of Russia's willingness to employ cyber capabilities to disrupt defensive military operations and sow discord. Another concerning trend is Russia's cooperation with Iran on cyber. For example, in March 2023, Russia sent Iran digital surveillance software, and Tehran is seeking more assistance from Russia.

Other Persistent Threats

Following Hamas's attack against Israel on October 7th of last year, Iran has exploited cyberspace to create additional disruptions and challenges in Israel. Iran recently used an online persona to claim credit for malicious cyber activity targeting Israeli-made devices commonly used in the water and wastewater sectors, impacting multiple victims in the United States. While many of these malicious cyberspace activities have been relatively limited in their impact, the ability of both state and non-state actors to act against Israel in the immediate aftermath of the Hamas attack is a reminder of what to expect in future conflicts.

The Democratic People's Republic of Korea's (DPRK) cyber actors remain intent on stealing and acquiring cryptocurrency to generate revenue for the regime's weapons of mass destruction and ballistic missile programs. The DPRK was responsible for the theft of hundreds of millions of dollars in cryptocurrency last year and continues to seek opportunities to leverage commercial firms to facilitate its laundering of stolen funds.

Additionally, the United States continues to face the still-growing threat posed by for-profit cyber criminals that target a wide array of vulnerable sectors, conducting ransomware attacks that impact the daily lives of Americans across the country. The recent ransomware attack against Change Healthcare was one of the most damaging that the United States has seen, with both tangible and psychological impacts that influence the implicit trust Americans have in their medical providers. This type of reckless and indiscriminate targeting of civilian sectors that threaten people's lives and livelihoods is unacceptable.

2023 Defense Cyber Strategy

In response to these evolving challenges, the Department developed and the Secretary approved DoD's fourth Defense Cyber Strategy last May. This strategy, along with its unclassified summary, highlights the importance of defending forward, disrupting malicious cyber activity before it can pose risk to our Homeland, and of strengthening partnerships with Allies and partners and our Defense Industrial Base (DIB) to bolster cybersecurity efforts. The 2023 Defense Cyber Strategy builds upon years of experience conducting offensive and defensive cyberspace operations, reflecting the Department's commitment to preemptively countering cyber threats and operationalizing the priorities outlined in the 2022 National Security and Defense Strategies.

The 2023 Defense Cyber Strategy was issued at a pivotal moment as the Department prioritizes the challenges posed by technologically advanced, near-peer adversaries. The strategy draws on lessons learned from Russia's 2022 further invasion of Ukraine, which has prompted a global reconsideration of the role of cyber in conventional conflict. These events reaffirmed that war-time cyberspace operations are best understood as a complement to conventional missions rather than as a decisive standalone capability.

Russia's cyber operations in the war in Ukraine are largely consistent with the strategic miscalculations we have observed with Russia's kinetic forces. The Department does not consider this to be proof of the weakness of Russia's cyber arsenal or a failure of cyber as a tool in warfare. Rather, we assess that it is a reflection of the challenges of integrating multi-domain operations and Ukraine's resilience, which has been reinforced by strong support from the international community and private sector partners.

Strategic Lines of Effort in Cyberspace

As we stand on the brink of what President Biden has called the "decisive decade" that will determine the shape of the strategic environment to come, DoD will seize the moment to fortify our cyber resilience and invest in our people. To that end, we continue to work across government stakeholders to execute on four lines of effort: Defend the Nation; Prepare to Fight and Win the Nation's Wars; Protect the Cyber Domain with Allies and Partners; and Build Enduring Advantages in Cyberspace.

Defend the Nation

First, we are actively campaigning in and through cyberspace to identify and mitigate cyber threats and their supporting ecosystems before they can harm the American public. In the Department, we call this "defending forward," meaning proactively disrupting malicious cyber activity to deny benefits and raise costs for adversaries. We do so by working closely with our partners in other Departments and Agencies to enable the defense of U.S. critical infrastructure and the DIB and to counter threats to military readiness. The Department has the capability to leverage offensive cyberspace operations, when necessary, with the agility and speed needed to address ever evolving foreign cyber threats in an exceptionally volatile domain. Additionally, the Department will continue to leverage operational insights gained from engagement with adversary cyber actors to bolster U.S. cyber defenses and inform the risk management approach of the Defense enterprise.

Prepare to Fight and Win the Nation's Wars

Second, the Department continues to leverage cyberspace operations to enable and empower Joint Force objectives, operating within the framework of persistent engagement to maintain constant pressure on adversaries. The Department campaigns consistently below the level of armed conflict to maintain the capability to leverage the digital domain to gain a decisive advantage in relevant conflicts. We will improve the resilience of the Department of Defense Information Network (DoDIN) and support campaign and contingency planning for joint plans and operations to reinforce both our defensive and offensive capabilities. As the Department campaigns in cyberspace for these purposes, we will develop offensive and defensive options to support the Joint Force so that it remains ready to respond rapidly across the spectrum of conflict.

Protect the Cyber Domain with Allies and Partners

Third, we are investing in our greatest asymmetric advantage – our global network of Allies and partners. Because of the interconnected nature of cyberspace, U.S. adversaries often target Allied and partner networks in order to gain access to our U.S. systems. Additionally, adversaries may test cyber tools and capabilities on partner nations, providing unique insights into adversary cyber force tactics, techniques, and procedures (TTPs) that can improve U.S. defenses against similar operations. This means that helping boost Allied and partner cybersecurity isn't just a "nice to have" – it is a national security imperative. The 2023 Defense Cyber Strategy commits to building the capacity and capability of U.S. Allies and partners in cyberspace and expanding avenues of cooperation to allow for timely information sharing and interoperability.

Hunt Forward Operations conducted by USCYBERCOM remain a key component of how the Department works with Allies and partners in cyberspace, helping to identify vulnerabilities to their networks, which in turn bolsters U.S. cyberspace defenses. We intend to continue investing in these missions, taking a collective approach to cybersecurity with the goal of frustrating the objectives of adversary cyber actors.

DoD will continue bilateral technical collaboration to identify malicious cyber activity on Allied networks while promoting responsible state behavior in accordance with international law and cyberspace norms. For example, the Department has reinforced its strong information sharing relationship with Ukraine and continues to provide defensive support to enable the resilience of Ukrainian networks. We also recognize that reinforcing responsible state behavior in cyberspace requires engagement on issues of strategic stability even with countries with whom no cyber cooperation exists in order to prevent miscalculation. Last year, the Department hosted a working level meeting with PRC defense officials to discuss the tenants of the 2023 DoD Cyber Strategy unclassified summary, in accordance with the 2014 U.S.-PRC Memorandum of Understanding on Notification of Major Military Activities Confidence Building Measure Mechanism. By promoting responsible state behavior in cyberspace, building capacity and capability among our Allies, and fostering information sharing, we strengthen our collective defenses against cyber threats.

Build Enduring Advantages in Cyberspace

Finally, the Department is pursuing institutional reforms to build enduring advantages in cyberspace. Our people are our greatest cyber asset. The Department will prioritize reforms to improve recruitment, retention, and training of the Cyberspace Operations Forces (COF) and Service-retained cyber forces. We will equip our warfighters with the essential tools and technologies to adapt and respond continually to the emergent threats and changing technologies that we will face and prevent malicious cyber actors from achieving their objectives in and through cyberspace. Finally, the Department will prioritize necessary reforms to meet the intelligence needs of the cyberspace operations community.

Posture Review

Looking ahead, we are committed to implementing our strategy and monitoring progress through the forthcoming Cyber Posture Review in FY 2026. Since the last Cyber Posture Review was concluded in 2022, the Department has not only delivered the 2023 DoD Cyber Strategy but also has placed increasing emphasis on the quality of enterprise-wide data collection and begun streamlining data-driven analysis in collaboration with organizations such as the Chief Digital and Artificial Intelligence Office (CDAO) and the Analysis Working Group (AWG). These efforts will shape how we monitor the success of our implementation of the 2023 DoD Cyber Strategy and the readiness of the COF through meaningful metrics, improved reporting systems, and modern analysis tools. My office is currently working alongside CDAO and the AWG to develop an improved metrics and data governance structure for the next Cyber Posture Review. This enhancement will provide more accurate, relevant, and traceable analysis, enabling continuous improvement in our cyber capabilities and readiness.

Looking Forward in 2024

With an eye towards the future, we understand that the Department cannot advance its defense priorities without a ready, capable, and informed Joint Force, one prepared to operate as fluently in cyberspace as any other joint warfighting domain. To achieve this end, we will invest in our people, capabilities, and information needs to support and enable the full range of cyber activities.

People

The Department continues to view its people as the most critical driver of success in the cyberspace domain. The need to recruit, retain, develop, and reward service members and civilians with technical aptitude and skillsets becomes increasingly critical and challenging every year. In response to readiness challenges and incorporating input from Congress, the Department is continuing to execute a review and re-design of the COF. The aim of these efforts is to build a force that can gain operational advantage over our adversaries and competitors, maintain agility in conducting operations from competition to conflict, and recruit and retain the talent necessary for achieving the Nation's cyber missions.

The Department has both completed and is conducting several studies evaluating force generation, readiness, and force employment models for the COF. These reviews highlight the need to think boldly about changes to a force structure that has remained largely static since 2012 when the Cyber Mission Force was created. We are looking holistically at how to evolve the COF, focused on the mission sets of USCYBERCOM, and exploring models beyond iterative adjustments to the current approach. The Office of the Secretary of Defense, in partnership with USCYBERCOM, is refining options for the Secretary to improve how forces are presented to the Command, raise readiness levels of the force, and streamline support mechanisms to other Combatant Commands. The recommendations to the Secretary will further allow USCYBERCOM to exercise its authorities in partnership with my office.

Capabilities

I appreciate the recent budget authorities granted to USCYBERCOM and the Principal Cyber Advisor, and I look forward to supporting the Department's implementation, in partnership with General Haugh, of those authorities. Beginning in FY 2024, consistent with the

National Defense Authorization Act (NDAA) for FY 2022, the Commander of USCYBERCOM's authority to control and manage the execution of current cyber resources to man, train, equip, and operate the Cyber Mission Force is now expanded to include the planning, programming, and budgeting of future years' cyber resources. In addition, consistent with the authorities granted to the PCA in the NDAA for FY 2023, the ASD for Cyber Policy, as the PCA, will continue to review the proposed budgets of DoD components to ensure adequate resourcing for the cyber mission.

As part of the FY 2026 budget cycle, DoD released the first Department-wide Cyber Operations Programming Guidance, which will shape future investments in cyberspace operations capabilities across the FY 2026 – FY 2030 Future Years Defense Program (FYDP). This will serve as a rubric for certification of the Department's – and in particular USCYBERCOM's – future budget requests beginning in the FY 2026 cycle.

The FY 2025 Cyber Activities budget aligns with the 2022 NDS and reaffirms the Department's three enduring cyberspace missions: Defend the DoDIN, Defend the Nation, and Prepare to Fight and Win the Nation's Wars. To execute on these missions, the Department will invest in cyber capabilities supporting integrated deterrence, campaigning, and efforts to build enduring advantage including by overseeing investments across the DoD cyber community.

The Department will continue to build on the pathway laid out by the 2023 DoD Cyber Strategy and other initiatives established in past fiscal years to provide a stronger cyber posture through ongoing development, deployment, sustainment, and modernization investments in DoD cybersecurity tools and capabilities. The President's FY 2025 Budget includes $14.5 billion for cyberspace activities which encompasses: 1) cybersecurity; 2) cyberspace operations; and, 3) cyber research and development (R&D) activities, aligning DoD's commitment to strengthening its cyber capabilities and protecting its critical networks and systems from evolving threats.

1) Cybersecurity

The DoD Chief Information Officer (CIO) is responsible for certifying the $7.4 billion cybersecurity portion of the President's FY 2025 Budget, and I look forward to partnering with the DoD CIO to prioritize investments in areas across the Department's information and operational technologies including weapons systems, defense critical infrastructure cybersecurity, supply chain risk management, DIB security, and key management infrastructure modernization. Additionally, DoD is building cyber resilient platforms to execute kinetic and non-kinetic missions by implementing the Strategic Cybersecurity Program, providing and assessing vulnerability mitigation plans, cryptographic modernization plans, and defensive monitoring recommendations. The Department is also transitioning to Zero Trust under the leadership of the DoD CIO, who is driving cybersecurity architecture planning, encryption modernization, and risk management of legacy Information Technology and weapon system cybersecurity.

2) Cyberspace Operations

The President's FY 2025 Budget requests $6.4 billion for Cyberspace Operations, including nearly $3 billion in annual budget authority for USCYBERCOM offensive and defensive cyberspace operations programs and activities, force generation and readiness, and capabilities and infrastructure directly supporting joint operations. Priority investment areas include manning, training, and equipping the CMF and advancing capable dual-use cyber ranges and testing facilities to support full spectrum multi-domain operations. The budget further prioritizes optimized equipment for hunt forward and enhanced sensing and mitigation operations and building out the Joint Cyber Warfighting Architecture (JCWA), which encompasses many capabilities that support operations from competition through conflict. The budget prioritizes support for Indo-Pacific and European theater priorities and identifies cyberspace information collection and analysis as a critical need to enable U.S. cyber forces to prepare for and conduct offensive and defensive cyber effects operations and joint training.

3) Cyber R&D

Finally, the FY 2025 Budget requests $629 million to support advanced R&D of new capabilities. The Cyber R&D budget will propel the Department's cyber programs forward by modernizing existing capabilities while advancing next generation tool development in support of Departmental cybersecurity and cyber operations programs. These efforts focus on developing the computing, networking, and cybersecurity technologies required to protect DoD, U.S. Government, and civilian information, infrastructure, and mission-critical systems and are crucial to accelerating efforts across the Department to implement the 2023 DoD Cyber Strategy. Over the next fiscal year, DoD will conduct further demonstrations and evaluations with warfighters, acquisition programs, and combatant commands to assess and improve prototype utility.

Information

Undergirding all of our work to develop capabilities to ensure overmatch against U.S. adversaries is the need for timely and accurate information to inform our operations. The 2023 DoD Cyber Strategy places renewed emphasis on the role intelligence plays in the planning and execution of cyberspace operations. The Office of the Under Secretary of Defense for Policy is working closely with the Office of the Under Secretary of Defense for Intelligence and Security, and through them, the Defense Intelligence Enterprise, to ensure that the intelligence requirements of the cyber warfighter are prioritized. The Department will improve business practices and human capital management processes to expand cyber intelligence production and reduce barriers to information sharing consistent with applicable law, policies, and procedures. Consistent with the notification to the Committee by the Secretary, Chairman of the Joint Chiefs of Staff, and Director of National Intelligence, the Dual Hat leadership arrangement, whereby the position of the Director of the National Security Agency and the Commander of USCYBERCOM are held by the same official, is critical to ensuring that our intelligence and military activities are properly integrated.

Conclusion

In conclusion, cyberspace and technology continue to evolve precipitously, requiring the Department and the United States more broadly to anticipate changes and move with the speed and agility necessary to stop those who seek to exploit it. The Department will execute on the path established in the 2023 Defense Cyber Strategy to protect the shared digital environment from those who intend to subvert our values and interests. By pursuing integrated deterrence, which includes our cyber capabilities, the Department will be ready to fight and win the Nation’s wars with an ability to respond rapidly across the spectrum of conflict. The Department will make full use of the authorities and capabilities Congress has provided to us as we continue to deter aggression and defend our Nation’s security. Thank you for your continued support in this fight and I look forward to answering your questions.