STATEMENT OF

THE HONORABLE DR. JOHN PLUMB

ASSISTANT SECRETARY OF DEFENSE FOR SPACE POLICY

TESTIMONY BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION

MARCH 30, 2023

Introduction

Chairman Gallagher, Ranking Member Khanna, and distinguished members of the Committee: Thank you for inviting me to testify before you on the Department of Defense's cyber posture and the progress we have made in achieving our objectives in cyberspace. I am pleased to appear alongside General Nakasone.

Today, the United States faces diverse threats both internal and external to cyberspace. As Secretary Austin has said since his first days in office, the People's Republic of China (PRC) is the Department's pacing challenge and Russia remains an acute threat. This is as true in cyberspace as it is in other warfighting domains. Other persistent threats arise from North Korea, Iran, and transnational criminal organizations—many of which work to tacitly advance the interests of their host nations. These adversaries use cyberspace to conduct malicious cyber activity (MCA) against the Department of Defense Information Network (DODIN) and U.S. homeland, weaken Allies and partners, and undermine U.S. values, institutions, and interests.

The Department has long recognized the dangers inherent in the cyber domain and has maintained efforts to protect its own systems. Since 2018, the Department has recognized that it is not enough to maintain a defensive posture while preparing for conflict, but that it must defend forward to meet adversaries and disrupt their efforts to conduct MCA against the United States during competition.

The Department campaigns in and through cyberspace to sow doubt among competitors; conducts intelligence-driven hunt forward operations in order to generate insights into competitors' tactics, techniques, and procedures (TTPs) while defending U.S. Allies and partner computer networks from MCA; and disrupts malicious cyber actors through offensive cyber operations. The Department is also seeking to enhance capacity building efforts with U.S. Allies

and partners – a strategic force multiplier and asymmetric advantage that our competitors cannot match.

The Department is building enduring advantages in the cyber domain. The President's Fiscal Year (FY) 2024 budget request includes $13.5 billion for cyberspace activities, an increase of $1.8 billion from the enacted level in FY 2023, which will enhance the Department's cybersecurity, increase capacity for cyberspace operations, and advance research and development activities for new cyber capabilities. In particular, the FY 2024 President's budget requests $7.4 billion dollars for cyberspace operations, including nearly $3 billion for United States Cyber Command (USCYBERCOM). These resources will go directly to supporting our cyber mission forces, protecting the homeland, and addressing the threats posed by our adversaries in cyberspace.

Security Environment

China

For decades, the PRC has used its cyber capabilities to steal sensitive information, intellectual property, and research from U.S. public and private sector institutions, including the defense industrial base (DIB). In 2022, the Federal Bureau of Investigation (FBI) publicly attributed to PRC state-sponsored cyber actors malicious cyber activities that targeted at least six U.S. states, gathering health, transportation, and other sensitive information. Hackers linked to the PRC government have stolen COVID relief funds, conducted ransomware attacks, and collected private information and data about American citizens to benefit their espionage efforts. The PRC's vision for the future is a world where it dominates – economically, ideologically, and

militarily – and the PRC is developing and integrating cyber capabilities to make that vision a reality. In a crisis, PRC leaders believe that achieving information dominance will enable them to seize and keep the strategic initiative, disrupt our ability to mobilize, project, and sustain the Joint Force; and ensure their desired end-state. PRC cyber intrusions are already the most prolific in the world and show no signs of slowing down.

Russia

Russia engages in persistent MCA to support its global espionage campaigns, steal intellectual property, disrupt critical infrastructure such as energy and logistics networks, promote disinformation, and undermine democratic processes. Russia also views cyber operations as a key component of its wartime strategy. The MCA against Viasat, a U.S. satellite company, at the outset of Russia's further invasion of Ukraine in early 2022 showcased how Russia uses cyber operations to degrade the command and control of the Ukrainian forces and enable Russian maneuvers.

Iran, the Democratic People's Republic of Korea (DPRK), and For-Profit Actors

Iran regularly uses cyberspace operations to engage in both espionage and criminal activity. In 2022, Iran engaged in a reckless and irresponsible MCA against Albania, disrupting public services, damaging critical infrastructure, attempting to erase critical data and state records, and threatening our ally's security. Iran also regularly conducts MCA against U.S. critical infrastructure and has engaged in cyber-enabled influence campaigns to target American voters with misinformation.

The DPRK continues to use its cyber capabilities to steal information and resources, including stealing cryptocurrency to illegally generate revenue for the regime and support its weapons of mass destruction and ballistic missile programs. Earlier this year, the FBI accused DPRK hackers of stealing $100 million in cryptocurrency in June 2022, in addition to the roughly $600 million stolen in March 2022.

U.S. interests in cyberspace are also threatened by profit-motivated transnational criminal organizations: ransomware gangs, hacktivists, and state-sponsored cyber mercenaries. Their targets include both the DIB and U.S. critical infrastructure. Whether these criminals operate independently of, are tacitly tolerated by, or are actively encouraged by nation states, they represent a threat to national security. The rapid increase in volume and scope of ransomware activity threatens both the American people and our economy, and it requires a whole-of-government effort to counter and mitigate threats.

Strategy

In 2022, the Department conducted its second Quadrennial CPR, which the Secretary signed and delivered to Congress in January 2023. The focused evaluation of Cyberspace Operations Forces and critical enablers provided a measure of mission progress since 2018 and underscored the persistent challenges in the face of fundamental changes in the global cyberspace environment in recent years. The CPR highlighted how the Department's cyberspace mission can advance strategic objectives through increasingly integrated, agile, and data-driven processes to boost readiness of effectively aligned, trained, and equipped operational cyber forces. The findings of the CPR – which encompass areas of force generation, capability

development, intelligence support, planning and budgeting, and operational processes – serve as the substantive basis of the Department's strategy in cyberspace.

In the coming years, the Department will operationalize the 2022 National Defense Strategy objectives for cyberspace of integrated deterrence and campaigning. Following decades of focus on counterterrorism while the cyber domain has undergone rapid growth, the Department today is underinvested in cyber. The Department must invest to deepen the integration of cyber into our warfighting capabilities. In addition, we cannot overstate the importance of U.S. Allies and partners as a strategic advantage and force multiplier in cyberspace and captures the necessary force generation and intelligence reforms to build enduring advantages.

Investments

The National Defense Strategy (NDS) recognizes that the Department cannot achieve its deterrence objectives without a ready, capable, and informed Joint Force that is equipped to operate in contested environments. Cyberspace operations are core to the concept of integrated deterrence and the Department is focused on establishing and maintaining enduring advantages that support and enable the full range of cyber activities. In particular, the Department is deliberately shaping and resourcing efforts to meet the needs of its operational commanders. The President's FY 2024 budget request prioritizes investments in all aspects of cyberspace – in our people, organization, operations, intelligence, and capabilities.

Over the last several years, USCYBERCOM has assumed a greater "service-like" responsibility and authority for Cyberspace Operations Forces. The Office of the Principal Cyber Advisor's team and USCYBERCOM have been preparing the actions and processes needed for directly controlling and managing the Planning, Programming, Budgeting, and Executing of the

resources to train, equip, operate, and sustain the Cyber Mission Force starting in FY24, as directed by Section 1507 of the FY 2022 National Defense Authorization Act (NDAA). The Department's transfer of budgetary authority to USCYBERCOM further enables the Cyberspace Operations Forces and addresses the critical cyberspace mission priorities in the 2022 National Defense Strategy. The President's FY 2024 budget request includes nearly $3 billion for USCYBERCOM, an increase of over $750 million from the enacted level in FY 2023, which is primarily aligned to four priorities:

- Cyberspace Operations Forces Readiness and Training ($308M in FY 2024)
- Defending and Protecting the DODIN ($309M in FY 2024)
- Support to the Combatant Commands and key Allies and partners ($549M in FY 2024)
- Joint Cyber Warfighting Architecture (JCWA) Development and Integration ($1,294M in FY 2024)

Cyber Operations Forces Readiness and Training

The Cyber Operations Forces readiness and training is the foundation for all the Department's joint cyberspace operations capabilities. The FY 2024 budget request includes $308 million, an increase of $98 million from the enacted level in FY 2023, for USCYBERCOM to advance the training and readiness of the cyberspace operational force, including the further development and expansion of Persistent Cyber Training Environment (PCTE). This separate, dedicated funding for the joint cyber force will provide a secure training and real-world operating environment that simulates threat cyberspace and provides high-fidelity mission rehearsal, provides for improved exercises, and develops advanced cyber institutional training

for the entire joint force.

Defending and Protecting the DODIN

The Department continues to prioritize protecting the DODIN through support to USCYBERCOM's defensive cyberspace operational forces and their ability to respond to malign cyber activity. This effort includes enhancing the cybersecurity of DODIN enterprise networks, weapon systems, information, and defense critical infrastructure. In FY 2024, the President's budget requests $309 million, an increase of $67 million from the enacted level in FY 2023, for defending the DODIN through additional sensors, mitigating cyber vulnerabilities to Defense critical infrastructure, exporting defensive cyber capabilities through increased security cooperation, and prioritizing cyber protection for critical nodes for defense of the homeland. The budget includes funding for hunt forward operations for intelligence-driven threat hunting for advanced persistent threats that have been proven successful both for U.S. support to Ukraine against Russian MCA and our Cyber Protection Teams' efforts globally.

Support to the Combatant Commands and key Allies and partners

The President's FY 2024 budget request supports U.S. Combatant Commands, Allies, and partners through increased emphasis and investments in operational partnerships, increasing alternative and off-net access capabilities, expanding intelligence and technology, and exporting effective cybersecurity protocols and techniques through improved security cooperation. The budget requests $549 million in FY 2024 for this support, an increase of $161 million from the enacted level in FY 2023, including alternative access and niche cyber weapons capabilities investments. These investments will improve cyber support to critical Indo-Pacific and European

Combatant Command plans, initiatives and programs.

JCWA Development and Integration

USCYBERCOM's JCWA is the foundational concept and architecture for cyber infrastructure and development into a "joint cyber weapons platform" for conducting its Title 10 joint cyberspace operations, and it will immediately benefit from USCYBERCOM's new programmatic, budgetary, and acquisition oversight. The President's FY 2024 budget requests $1.294 billion for JCWA capabilities investment, an increase of $403 million from the enacted level in FY 2023, to enable JCWA program executive and integration efforts, improved cyber weapons and multi-use hardware and software tools, ensuring the interoperability of service-developed programs and big data platforms, the viability of JCWA future spiral capability and development, and the prioritization of funding to operationalize and speed development of this capability.

Operations

Under the existing national policy framework for cyber operations, the Department is able to conduct timely offensive cyber operations when threats meet the threshold for action. This authority is critical to the Department's ability to leverage cyberspace with the speed and agility required to support national security objectives.

Campaigning and Hunt Forward

Campaigning in and through cyberspace is key to our goal of advancing Joint Force objectives. Campaigning complements the Department's existing posture in cyberspace and has

been applied to defeat other malicious actors including those intending to influence U.S. elections and disrupt our way of life via ransomware.

The Department has integrated cyberspace operations in its campaign and contingency planning. We plan to further refine this approach and utilize the unique characteristics of cyberspace to meet the Joint Force's requirements and generate advantages in support of combatant commanders. We are developing options to degrade the cyber capacity of U.S. adversaries and prevail across the continuum of competition, crisis, and conflict.

Campaigning also aligns with the concepts of defend forward and persistent engagement. The Department is defending forward by disrupting the activities of malicious cyber actors and degrading their supporting ecosystems. These operations are primarily conducted by USCYBERCOM, leveraging its authorities and in close coordination with other government departments and agencies as well as our Allies and partners. Lessons learned from these operations inform our pursuit of new capabilities and shape our approach to risk management.

Hunt forward operations assist in the defense of U.S., Allied, and partner networks, mitigating harms and disrupting malicious cyber actors. Hunt forward operations conducted by USCYBERCOM have led to strong information-sharing relationships with a number of foreign partners, including Ukraine. They have enhanced U.S. cybersecurity preparedness, contributed to the readiness of the Joint Force, and exposed hostile TTPs. They have also bolstered the resilience of Allies and partners.

These operations also support the strategic approach outlined in the 2023 National Cybersecurity Strategy, in which the Department's cyberspace operations may complement concurrent actions by the diplomatic, law enforcement, and intelligence communities, among

others. Together, these actions support a whole-of-government effort to reduce the perceived and actual utility of MCA and render cybercrime unprofitable.

Securing and Defending the DODIN

To deter aggression and prevail in conflict, when necessary, the Department must demonstrate its resilience to adversary MCA and its readiness to operate in contested cyberspace. This starts with securing and defending the DODIN, which comprises all of the Department's electronic information systems and associated processes used to collect, process, store, transmit, disseminate, and manage digital information. The DODIN includes mission-critical information technology and weapons systems and critical infrastructure interacting with the DODIN that are owned, operated, or leased by the Department. Cyber resilience and survivability are foundational to integrated deterrence.

To achieve the required resilience, the Department is implementing Zero Trust architectures and associated cybersecurity technologies, modernizing its cryptographic algorithms and technologies, and strengthening cybersecurity in the DIB. The Department is also prioritizing new technologies that may confound malicious cyber actors and prevent their exploitation of the DODIN. These include advanced endpoint monitoring capabilities, tailored data collection strategies, automated data analytics, and systems that enable network automation, network restoration, and network deception.

Intelligence

Close coordination between the Department and the Intelligence Community is vital to maintaining U.S. superiority in the cyber domain and protecting our national security interests. In

particular, the Dual Hat leadership arrangement, in which the positions of the Director of the National Security Agency and the Commander of USCYBERCOM are held by the same official, has ensured that our intelligence and military activities in this critical domain are integrated and we are best positioned to work alongside our allies and partners. To ensure our assessment of this arrangement reflects the most current information, last year the Secretary and the Director of National Intelligence directed a joint study of the Dual Hat leadership arrangement. Informed by this study, DoD and ODNI are building a roadmap and will brief the roadmap to Congress once it is complete.

Intelligence support to cyber resilience and operations

Part of our mission is to identify MCA early in their planning and development and persistently engage U.S. adversaries in cyberspace. In coordination with the IC, we can track the organization, capabilities, and intent of malicious cyber actors—insights we use to bolster cyber resilience and when circumstances permit, share relevant information with non-governmental stakeholders.

Intelligence support for cyber operations will become ever more critical as this domain takes on a more significant role in warfare. The Department is prioritizing necessary reforms to meet the intelligence needs of the cyberspace operations community. The Department is incorporating requirements for the cyber domain into the business practices, human capital management, and organization of the Defense Intelligence Enterprise.

Information Sharing to improve cybersecurity

The Department is the Sector Risk Management Agency for the DIB, which develops, manufactures, and maintains sensitive technologies vital to the defense of the Nation. Through the DIB Cybersecurity Program, the Cyber Crime Center's DoD-DIB Collaborative Information Sharing Environment (DCISE), and the NSA's Cybersecurity Collaboration Center (CCS) and Enduring Security Framework (ESF), the Department has invested in the defense of the DIB through near real-time information sharing and operational collaboration. At the core of these efforts are our deep and transparent relationships with the private sector and other non-Federal stakeholders and sharing contextualized threat information that helps industry partners identify and prioritize threats. Continuing to build on these partnerships will be critical, as voluntary collaboration is the foundation of our multi-pronged approach for ensuring the cybersecurity of the DIB. Consistent with the 2023 National Cybersecurity Strategy and recommendations from the Cyberspace Solarium Commission, the Department will also partner with DHS and other agencies to improve the cybersecurity of non-defense sectors that impact national security. Through these efforts focused on information sharing, we provide threat information to the private sector to enable them to protect themselves.

People

The Department's most important cyber capability is its people: those with the talent, creativity, and sense of mission necessary to defend the Nation in cyberspace. Existing manpower models and processes are optimized for the development and management of general-purpose forces, but cyberspace operations demand technical expertise, target- and network-specific knowledge, and rigorous training. Recruitment and retention remain a major challenge for the Department.

Force generation study

Addressing training and readiness challenges requires innovation in force generation and management policies. Consistent with the findings of the recently completed CPR, any solution to this problem set will require reforms across the spectrum of cyberspace operations and lifecycle of the cyber workforce as an integrated solution. To that end, and to generate enduring advantages that enable its operations in cyberspace, the Department is undertaking a strategic force generation and readiness reform effort focused largely on the Services' force development and management policies and USCYBERCOM's execution of its Service-like responsibilities.

As directed by Sections 1533 and 1537 of the FY 2023 NDAA, the Department is initiating a formal study to assess diverse alternatives for organizing and training the cyber operations forces. I would like to thank the Committee for giving us both the time and resources to dedicate to this critical issue. The Office of the Secretary of Defense, USCYBERCOM, other Unified Combatant Commands, and the Military Departments are involved in this study. The results will drive necessary changes in the force generation and management policies, processes, resources, and constructs that govern or support the cyber operations forces, thereby improving these forces' readiness and optimizing them for execution of USCYBERCOM's critical missions.

Cyber training and awareness

The Department is enhancing the cyber resilience of the Joint Force by ensuring its ability to fight through network degradations. Cyberspace operations may be the responsibility of

a relatively small number of cyber professionals, but cyber risk is a challenge shared across the defense enterprise. The Joint Force relies on cyberspace to execute its missions and operate across the continuum of competition, crisis, and conflict. As a result, the Department is taking action to foster a culture of cybersecurity and cyber awareness. We are investing in training to ensure that service members of all ranks are appropriately informed about key cyber issues, including by incorporating cyber education requirements into curricula at the service academies, in reserve officer training corps programs, and in enlisted training programs.

Allies and Partners

U.S. Allies and partners are a force multiplier in cyberspace and an enduring, asymmetric advantage that no competitor can match. Integrated deterrence requires an alignment of capabilities with those Allies and partners with whom the United States shares common interest and values as well as deep interoperability with those most highly capable. The NDS directs the Department to incorporate Allies and partners at every stage of defense planning, and this is the case in the cyber domain.

The Department's engagement with Taiwan illustrates our efforts in partner capacity building in cyberspace. In partnership with Taiwan's Ministry of National Defense, under the auspices of the American Institute in Taiwan (AIT) and the Taipei Economic and Cultural Representative Office in the United States (TECRO), we are working to help Taiwan develop effective cyber defenses along with threat detection and monitoring capabilities. The Department has also provided training and education courses, helped to develop its cyber defense institutions and modernize its networks, and provided tools for threat detection and defense.

The Department is enhancing relationships at the strategic, operational, and tactical levels with our most cyber-capable Allies and partners and is dedicating long-term work to develop the cyber capability and capacity of less capable partners. The DoD Cyber Crime Center, in coordination with USCYBERCOM, has developed and provided cyber mission force training for the United Kingdom, Canada, Australia, and New Zeeland and provided specialized cyber forensics training to other allied partners. Building on lessons learned from our partnership with Ukraine, we are emphasizing the timely sharing of information to increase the effectiveness of cyberspace operations and enhance collective cybersecurity efforts.

Conclusion

Successfully operating in cyberspace is essential to the Department's mission to provide the military forces needed to deter aggression and ensure our Nation's security. Our adversaries continue to extend and evolve their cyber capabilities, exercising them in competition and conflict to degrade our advantages and increase their own. The Department is committed to strengthening both our defensive and offensive cyber capabilities and maturing our cyber forces in partnership with this Committee. Thank you for your continued support for the Department and the Nation, and I look forward to answering your questions.