POSTURE STATEMENT OF

LIEUTENANT GENERAL WILLIAM J. HARTMAN, USA

ACTING COMMANDER, UNITED STATES CYBER COMMAND

BEFORE THE 119th CONGRESS

SENATE COMMITTEE ON ARMED SERVICES

SUBCOMMITTEE ON CYBERSECURITY

9 APRIL 2025

(U) Chairman Rounds, Ranking Member Rosen, and distinguished members of the sub-committee, thank you for your support and for the privilege of representing the men and women of U.S. Cyber Command (USCYBERCOM).

(U) I value this opportunity to discuss the changing strategic landscape, the Command's accomplishments in 2024, and the prospects ahead for us in 2025. USCYBERCOM creates an enduring advantage for the Joint Force, for the nation, and for its partners. Our Command is fostering a warrior ethos and lethality by building and sustaining mastery in our cyber forces. We are implementing national strategy and re-establishing deterrence by buying down risk for the Department of Defense (DoD), and by harnessing our Service-like authorities, such as Enhanced Budget Control. Congressionally granted authorities and oversight are crucial to USCYBERCOM's success, helping us to anticipate changes in the strategic environment, and to act with speed, scale, and agility.

(U) New technologies are changing the dynamics of cyberspace and the character of conflict. Cyberspace operations demand and reward agility and rapid capability development, and thus we require acquisition and programming processes that move at the speed of relevance. The unique authorities granted us by Congress allow USCYBERCOM to be ready, but this also means added expectations on our Command. I shall explain below how we are responding to this challenge.

(U) USCYBERCOM possesses operating, equipping, and sustaining responsibilities for the nation's joint cyber force. Each of the Armed Services develops and presents personnel to

our Cyber Mission Force (CMF). Each of the Service Cyber Component commanders also serves as a Joint Force Headquarters-Cyber commander executing missions in and through cyberspace. It is also important to mention here our direct-report components: our sub-unified command – the Cyber National Mission Force-Headquarters (CNMF-HQ) – along with our Joint Task Force Ares, and our Joint Force Headquarters-DoD Information Network (JFHQ-DoDIN). Congress recently directed the latter to be elevated to a sub-unified command under USCYBERCOM and that elevation will take place later this year. In addition, USCYBERCOM operates closely with Coast Guard Cyber Command, an element in the Department of Homeland Security (DHS). These components, in combination, provide robust capacity and capability for the Department of Defense and for the nation.

(U) USCYBERCOM, through its components, executes four assigned missions. The Cyber National Mission Force defends the nation from malicious cyberspace actors who threaten our critical infrastructure and democratic processes. Joint Force Headquarters (JFHQ)-DoD Information Network (DODIN) operates and defends the DODIN to ensure our warfighters can execute missions globally. Our service-led Joint Force Headquarters – JFHQ-C (Navy), JFHQ-C (Army), JFHQ-C (Marines), and JFHQ-C (Air Force) – integrate options and capabilities into Combatant Command campaigns and plans, posturing the command to support the Joint Force as we collectively re-establish deterrence against adversaries and prepare to win our nation's wars. Finally, we bolster the effectiveness of our allies and partners, empowering them to accomplish their missions as well as to assist the Department's efforts.

(U) The National Security Agency (NSA) is our Command's closest partner. I serve as both the Acting Commander of USCYBERCOM and the Acting Director of NSA. Every day I see how the Agency's roles, responsibilities, and unparalleled capabilities complement those of USCYBERCOM. The synergy between these two organizations drives a unity of effort that strengthens the Department, the Intelligence Community, and ultimately the nation.

(U) At USCYBERCOM, our Code is "We win with people." This guiding principle highlights our dedication to building a culture where initiative, innovation, collaboration, and the expertise of our personnel drive mission success. The people of USCYBERCOM are dedicated to defending our networks, countering threats, strengthening our partners, and providing a decisive advantage for policymakers and military commanders in competition and conflict. We amplify the impact of federal, military, foreign, and private-sector partner activities, synergizing the application of all instruments of national power against our adversaries. We are dedicated to ensuring our people have the necessary resources to optimize readiness and resilience as they face disproportionately large adversary forces.

(U) SHIFTING THREATS

(U) USCYBERCOM is in daily contact with determined and sophisticated adversaries, primarily state-sponsored cyber actors. DoD systems and data – as well as critical civilian infrastructure in the United States – have come under significant risk, while our responsibility to defend them remains a no-fail mission for the Department and the nation.

(U) We have witnessed bold efforts by state-sponsored cyber actors to achieve strategic objectives against the United States and its allies and partners. We focus on adversaries probing the DoDIN, U.S. weapons systems, and U.S. and Western critical infrastructure to hold vital economic and national functions at-risk. Adversary cyber actors also target Western defense industrial base networks to steal weapon-system technology.

(U) China is our pacing adversary. Beijing seeks a world order more in conformity with the Chinese Communist Party (CCP)'s vision and ideology – and Beijing views cyber as a critical domain for modern warfare . Not only is it our closest competitor in cyberspace; but it is also aggressively expanding its influence in the Pacific while insisting that it is only acting to defend itself. China employs the world's largest cyberspace operations workforce, supported by capable and adaptive enablers in its defense, cybersecurity, and information technology industries.

(U) Our Command gratefully acknowledges the importance that our allies and partners provide in defending our common interests and re-establishing deterrence in the Pacific. The United States cannot unilaterally match the quantity of resources that China can devote to cyber operations, but together we can exceed it in the quality of our people and our capabilities. That is the advantage that allies, partners, and industry provide us when we collaborate and synchronize efforts.

(U) Russia appears determined to continue its persistent threats to the peace of Europe and to the global order. Moscow violates international norms with its eleven-year old aggression

in Ukraine, coupled with its overt and covert attempts to intimidate Ukraine's supporters. As with China, Russia's sophisticated military and intelligence cyber forces actively support its strategic objectives. Russian cyber actors work to subvert Ukraine and divide the Western allies, seeking to undermine them both abroad and internally. In the Russian case, moreover, the Kremlin encourages, or at least tolerates, brazen cyber-criminal enterprises that often serve state purposes against foreign targets.

(U) Iran and North Korea sponsor increasingly capable cyber actors. We assess Iran seeks to increase penetration and targeting of industrial control systems to disrupt critical infrastructure in Israel and elsewhere. Pyongyang focuses its cyber actors on the circumvention of international sanctions and the generation of illicit revenue through cryptocurrency exploitation and IT workers. that likely supports the regime's nuclear weapons and ballistic missile programs.

(U) Non-state cyber actors remain a threat in cyberspace. Cyber criminals services continue to find new victims in the United States and globally. We are particularly concerned about the criminal enablers of such activities, such as those providing ransomware-as-a-service to all manner of bad actors. In addition, violent extremist groups still operate in cyberspace. Though their capabilities have been eroded, the Islamic State in Iraq and Syria (ISIS), al Qaida, and other terrorist groups maintain the intent to target Americans. Our Joint Force Headquarters-Cyber (Marines) works in conjunction with U.S. military and diplomatic efforts, supporting allies and partners who are disrupting terrorist propaganda and mobilization online as well as to provide critical intelligence.

(U) Cyberspace is a dynamically evolving domain that sees accelerating technological change. New technologies do not represent a direct threat in themselves, but they are nonetheless forcing every military and cyber force to adapt even more dynamically. That, in turn, is affecting our resources and organizational arrangements. Artificial intelligence (AI), of course, holds the potential to change the character of war. USCYBERCOM is leveraging AI to enhance our capabilities in collection, detection, exploitation, maneuver, and command and control, generating greater speed and scale. There is no inherent obstacle to our adversaries using AI for similar purposes – or even more. Automation and autonomy – in cases enabled by AI – are transforming ideas from theory into real and even disruptive weapons and tools on battlefields and in competition across the globe. Our allies, partners, and adversaries are all engaged and propelling this technological progress. I shall say more about our response in a moment.

DEFENSE OF THE NATION

(U) USCYBERCOM defends the nation against threats in and through the global and interconnected domain of cyberspace. This work begins with the defense of the DoDIN but extends directly and indirectly to government, critical infrastructure, and partner systems as well.

(U) Our Command guards the military systems and data that provide warning, situational awareness, synchronization, and sustainment for our fellow Combatant Commands in their geographic and functional areas of responsibility. This is our supported mission at USCYBERCOM. All of the Combatant Commands support our execution of it because every

Combatant Command's operational plan depends on the ability of leaders and commanders to communicate orders and data securely. USCYBERCOM's responsibility, executed in particular through JFHQ-DoDIN, includes working with the other Commands, with the DoD Chief Information Officer (CIO), and with the Defense Information Systems Agency (DISA) to identify key cyber "terrain" and ensure they – and we – have cognizance of its status as well as clearly defined roles and assignments for defending it. When necessary, our Cyber Protection Teams work with local network defenders to identify and expel would-be intruders on Joint Force and DoD systems.

(U) The Defense of the Nation is integral to re-establishing deterrence. USCYBERCOM is strengthening the defense of critical infrastructure and the DoDIN by investing in and implementing stronger, more proactive cybersecurity measures; investing in artificial intelligence and machine learning to improve threat detection, response times, and predictive analysis; enhancing the knowledge, skills, and the capabilities, of our workforce; leveraging new and existing authorities; and working with our Allies, partners, and industry to create a more difficult target for our adversaries.

(U) I am pleased to add here that we are increasing resources and focus of on behalf of the Combatant Commands directly engaged in defending the American homeland against other actors. This emphatically includes support for USNORTHCOM in securing our borders. We are also working with partners to counter foreign drug cartels. Our efforts should help make a difference against the flow of fentanyl as well. Finally, we support USSPACECOM and other DoD entities in bolstering defenses against missile attacks against the United States.

(U) USCYBERCOM dynamically employs our assigned forces to achieve multiple objectives and priorities. Our forces are tasked with safeguarding critical infrastructure and the DoDIN, conducting operations to disrupt, deny, and deter adversaries, and supporting joint operations worldwide. The employment of the cyber force is continually evolving in response to the shifting threat landscape and technological advancements. This demands effective coordination, robust intelligence, and a deep understanding of both the cyber domain and the broader geopolitical context.

(U) Our Command recognizes the vital role that we play in supporting the Joint Force in Pacific contingencies, focusing on the strategic and operational challenges that China presents in cyberspace. In particular, we assist USINDOPACOM in its mission to deter aggression and defend its area of responsibility. This commitment extends to the other Combatant Commands that would be involved in a Pacific crisis, particularly U.S. Transportation Command (USTRANSCOM), U.S. Strategic Command (USSTRATCOM), U.S. Special Operations Command (USSOCOM), and U.S. Northern Command (USNORTHCOM). We also work with U.S. Government partners and industry to counter China-based cyber threats to our homeland, allies, and partners. We are defending against Beijing's cyber operators persistent access to U.S. critical infrastructure systems pre-position for attack in a contingency or crisis scenario. We are also hardening DoD's cyber "terrain" across the Pacific region to make it more defensible against any attacker.

(U) USCYBERCOM supports U.S. Central Command (USCENTCOM) and USSOCOM in their work to re-establish deterrence and, if necessary, defeat Iran. With USCENTCOM, we

have helped bolster the cyber defenses of Israel and other regional partners. The Command has focused on securing key networks in the region, and provided actionable information, insights, and options to policy makers.

(U) Defending Joint Force and military systems and data parallels our efforts to support the defense of adjacent cyber terrain, particularly government, critical infrastructure, and partner networks. We work intensively across the Joint Force and with a variety of partners to do this – what we call "Setting the Globe" – because systems in one region often depend on the working and the security of other systems hundreds or even thousands of miles away.

(U) Our job is to work with an array of U.S. and foreign partners to ensure that adversaries cannot impair that connectivity or our decisionmakers' trust in its security. Foreign adversaries continuously update how they operate, and frequently work through (unwitting) American-owned networks and devices. USCYBERCOM seeks to foster unity of action across partners like the Service counterintelligence agencies, the Federal Bureau of Investigation (FBI)-led National Counterintelligence Task Force, and DHS's Cybersecurity and Infrastructure Security Agency (CISA), sharing actionable intelligence to counter adversary activities. In addition, USCYBERCOM and NSA enable efforts by the Department of the Treasury, the FBI, and other partners to disrupt ransomware, cryptocurrency theft, and other criminal activities, and vice versa.

(U) Consistent with Congressional intent, USCYBERCOM shares information with industry to help bolster private companies' ability to defend themselves against exploitation by

malicious cyber actors. We aim to broaden as widely as possible the sharing of insights that both our industry partners and we gain from this collaboration. Our UNDERADVISEMENT program, a voluntary collaboration with dozens of private partners, links cybersecurity expertise across industry and government. This partnership has cued significant operational successes, enabling network owners to close vulnerabilities and eradicate threats from their systems; this frustrates adversaries and makes their campaigns more expensive for them and less consequential for us.

(U) USCYBERCOM's Cyber National Mission Force (CNMF) conducts missions to counter malicious cyberspace activities, supporting all aspects of our defend-the-nation mission set. CNMF personnel have deployed more than 85 times to over 30 countries in partner-enabled missions to hunt on host networks. They conducted more than two dozen "hunt forward" missions in 2024, generating insights and constraining adversary freedom of maneuver. We conduct such missions in all Geographic Combatant Command regions. These missions have led to public releases of malware samples for analysis by the global cybersecurity community. Such disclosures have made Internet users around the world safer on-line, and frustrated the military and intelligence operations of authoritarian regimes. In addition, CNMF is leading our Command's effort to explore and apply artificial intelligence to the cyber mission set. The AI Task Force in CNMF already sees success in a growing series of pilot projects, which are having operational impact today.

BUILDING AND SUSTAINING MASTERY

(U) USCYBERCOM will create advantages for warfighters, the Department, our partners, and the nation in 2025, operating globally by enhancing readiness, implementing Service-like authorities, and advancing mission partnerships. I am pleased to report that all our Service cyber components have now attained foundational readiness standards across the forces they present to our Command. This objective, as you know, took years to achieve even with the dedicated efforts of the Services to improve the manning, training, and equipping of their respective forces. That milestone having been reached, however, we must now focus on what comes next. Readiness alone will not suffice given the magnitude of the task we face. Sustaining cyberspace operations at-scale against a determined and capable adversary that can build many more cyber elements than we can was a requirement not fully projected when the Department established USCYBERCOM in 2010 and authorized our Cyber Mission Force in 2012.

(U) Our response includes an initiative titled CYBERCOM 2.0, which we designed to foster mastery across the force so it can overmatch quantity with quality. The Department recently approved several concepts to update USCYBERCOM's force design and the ways in which it builds and sustains specialization and expertise in our teams. Together with the Services and our Components, we are crafting proposals to maximize capacity, capability, and agility, harnessing a stronger, more lethal force in more innovative and exciting ways. These include ways of fielding new technologies rapidly, finding ways to ensure they are tested and scalable. These steps were prompted and facilitated by recent National Defense Authorization

Acts' provisions on readiness and force generation that collectively gave the Department the opportunity to modernize the cyber force and reshape USCYBERCOM.

(U) Coupled with the readiness efforts highlighted above and organizational efforts to streamline the force, CYBERCOM 2.0 provides a pathway to maturation for the Command through the evolution to mastery. The initiative focuses on key enablers such as recruiting and retaining top talent, advancing training and education for the cyber force, and fostering an innovation ecosystem that moves at a mission-relevant pace, producing mission-relevant technologies. Overall, this results in a more experienced, better-trained, and better-equipped cyber force capable of adapting to the dynamic environment.

(U) Our cyber force aims to build mastery that in turn fosters speed and agility. In an environment transformed by AI and big data, operational and strategic advantage accrues to the side that sustains speed and efficiency in collecting and ingesting data, building and employing models and algorithms, and deploying and updating them at-scale—while also denying similar advantages to adversaries seeking to exploit our systems and data. We are focused on ensuring our data and analytic infrastructures deliver advantage, and that those systems attain sufficient resilience to function even under attack. Some of this work proceeds under the auspices of the DoD- and USCYBERCOM-developed five-year AI Roadmap, which guides the appropriate people, data, organizations, and infrastructure to deliver AI capabilities for all cyber mission sets; to counter AI threats and seize emerging opportunities; and to enable AI adoption.

(U) Strong partnerships with government, industry, academia, and foreign colleagues amplify our effectiveness and in turn create advantages for our partners. They force dilemmas upon our adversaries, and broaden the perspectives and insights we can utilize and exploit. Our Components, when working in unison with diplomatic, military, law enforcement, homeland security, and intelligence capabilities, make a powerful combination that can disrupt the plans of malicious cyber actors wherever they hide. In addition, our Regional Cybersecurity and Engagement Strategy in the Indo-Pacific guides efforts with partners to counter and contest foreign adversaries. Much of our effort at USCYBERCOM goes into fostering capacity building among partners, promoting interoperability, and reducing barriers to information sharing and combined activities.

(U) Congress enhanced our attractiveness to new partners by designating USCYBERCOM a federal lab for technology transfer. Why does that matter for a Combatant Command? Because as a lab, USCYBERCOM is authorized to sign Cooperative Research and Development Agreements (CRADAs) with industry and academic partners. We have reached several such agreements, allowing tighter collaboration between our operators and technical experts and, for example, local network defenders seeking to enhance their capabilities to detect whether their systems have been compromised. USCYBERCOM also has signed Education Partnership Agreements (EPAs) with several universities. Finally, our Academic Engagement Network (AEN) of more than 120 institutions is facilitating new partnerships and bringing fresh ideas to shared challenges.

(U) The Enhanced Budgetary Control (EBC) authority and resources granted in increments by Congress since 2018 are now hastening the Command's transformation. Fully implemented less than a year ago, this suite of authorities is already making a difference in our relations with DoD, the Services and our Components. EBC entrusts nearly $3 billion of the DoD budget to USCYBERCOM, and streamlines how we engage the Department's planning, programing, budgeting, and execution processes. EBC is promoting the transparency that facilitates tighter alignments between authorities, responsibility, and accountability in cyberspace operations. Greater accountability, in turn, facilitates better cybersecurity as well as faster development and fielding of new capabilities.

(U) We recognize that innovation is vital to achieving speed, agility, and scale across operations, capability deployment, data sharing, and procurement. Agile acquisition is crucial to creating advantage for our commanders, Components, and operators. The Command partners with the Services and DARPA (among others) to ensure our acquisition strategies achieve agility, scale, and precision at the rapid pace demanded by the cyber-domain. For example, USCYBERCOM partners with DARPA on an effort called CONSTELLATION to swiftly bridge the proverbial "valley of death" for new capabilities and rapidly transition emerging tools to the operational user.

(U) USCYBERCOM's new acquisition authorities promote agile methodologies for rapid AI development and iteration, enabling swift adaptation to evolving cyber threats and operational needs. Coupled with the Joint Cyber Warfighting Architecture (JCWA), the Command has a framework ensuring AI solution interoperability and integration across cyber domains. This

supports rapid prototyping, streamlined software acquisition, and the integration of commercial AI advancements.

(U) Key to speed and agility in operations is JCWA, a suite of systems with associated capabilities that facilitate a full spectrum of cyberspace missions and foster overmatch against sophisticated adversaries. Our Command is employing new systems engineering and integration authorities (granted by the Department) to oversee the fielding of JCWA and ensure it develops efficiently in accord with a common vision. By defining interoperability standards between the Service-managed subcomponents of JCWA, this has accelerated JCWA's interoperability, tool development capacity, and data flows within and across the Command and mission partners. Finally, the Department is working with USCYBERCOM to build our JCWA Program Executive Office (PEO), and ultimately to provide our Command with milestone decision authority for Service-managed JCWA programs of record.

(U) USCYBERCOM's efforts depend on the initiative, motivation, and excellence it sustains in its people. We must hire and retain key expertise, and keep our personnel ready to meet the challenges of competition and conflict in and through cyberspace. We are working to grow uniformed cyber leaders at all levels, up to and including the officers who will eventually succeed me in this post. The staffing and training of our teams improves every year, and the Command's cyber readiness system now ingests data directly from the Joint Staff's Defense Readiness and Reporting System (DRRS) without manual input. Furthermore, USCYBERCOM's authorities as Joint Cyberspace Trainer facilitates joint training standards

across the entire Department, boosting DoD's ability to defend networks while enabling CMF teams to focus on hunting and contesting foreign adversaries.

(U) Last year the Department of the Army took over the Combatant Command Support Agent (CCSA) role for USCYBERCOM. The Army's military and civilian leaders were superb in managing this transition and ensuring our civilians experienced a virtually seamless transfer. Department of the Army specialists are helping us fill our civilian billets, driving down security and personnel processing times, and we look forward to accelerating hiring actions to fill vacancies across the Command. We are using special hiring authorities offered in 10 U.S.C. 4092 to attract top technical talent to join USCYBERCOM, and look forward to hiring more experts in 2025. We are also maximizing use of DoD Cyber Excepted Service authority to streamline civilian hiring and offer competitive employment incentives.

(U) USCYBERCOM is exploring innovative ways to enhance our operations using the expertise resident in the National Guard and Reserves. We operate side-by-side daily with activated members of the Reserve Component integrated into our teams, and we collaborate with National Guard units on State Active Duty and State Partnership Program engagements. We look forward to expanding ways to make the Reserve Component integral to our efforts, and invite your ideas for doing so.

(U) Last year the Department established the Assistant Secretary of Defense for Cyber Policy as the Secretary's Principal Cyber Advisor to increase focus on cyber activities. The ASD will continue to be instrumental as USCYBERCOM implements new authorities and evolves to increase domain mastery and warfighting readiness.

(U) CONCLUSION

(U) USCYBERCOM creates advantage for the Joint Force, for the Department, for our partners at home and abroad, and most of all for the nation. We campaign in and through cyberspace to support national strategic goals in competition and set conditions for the Joint Force to prevail in crisis and win the nation's wars. We must do so faster and better in 2025 because the United States and our allies face increasingly sophisticated cyber threats from both state and non-state actors. We are meeting that need, and posturing our people and organization to accelerate their efforts. And we will proceed, of course, with scrupulous regard for the privacy and civil liberties of U.S. persons, and in an objective, non-partisan manner.

(U) Our operational experience reinforces the importance of campaigning globally in and through cyberspace across the conditions of competition, crisis, and armed conflict. The Command has authorities to set and validate requirements, to plan and execute programs, and to control budgets and resources. It is working with the Services to organize, train, and equip the force, and has achieved sustainable readiness levels. Its goal now is promoting mastery across our force, using the new resources and authorities Congress and the Executive Branch have provided. I am committed to creating a more lethal cyber force, operating with the speed, scale, agility, and precision that the cyber strategic environment demands.

(U) The men and women at USCYBERCOM are grateful for the support your Committee has given to our Command. Our Service members and civilians are the best I have encountered in my 36-year career, look forward to demonstrating how they can manage their responsibilities,

employ the resources that you have provided, and accomplish their missions to defend our nation. With continued strong partnership with Congress, I know we will succeed. Thank you, and now I look forward to your questions.