POSTURE STATEMENT OF

GENERAL TIMOTHY D. HAUGH

COMMANDER, UNITED STATES CYBER COMMAND

BEFORE THE 118TH CONGRESS

HOUSE COMMITTEE ON ARMED SERVICES

SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION

10 APRIL 2024

(U) Chairman Gallagher, Ranking Member Khanna, and distinguished members of the committee, thank you for your support and for the opportunity to represent the men and women of U.S. Cyber Command (USCYBERCOM). I am honored to appear beside the Honorable Ashley Manning, currently Performing the Duties of the Assistant Secretary of Defense for Cyber Policy.

(U) I appreciate the opportunity to discuss the current strategic landscape, the accomplishments of the Command in 2023, and the opportunities ahead in 2024. This is a year of opportunity for USCYBERCOM as we create enduring advantage for the Joint Force, our partners, and the nation. Our Command is maturing and innovating to perform its missions as threats and technology change. Authorities granted by Congress and the progress made by my predecessors are foundational to the Command's current and future success. Advantage in cyberspace goes to the entity postured to understand and anticipate changes in the environment and act on fleeting opportunities with speed, scale, agility, and precision. Understanding changes across the threat and technology landscapes will continue to drive Command initiatives.

(U) In that context, we have worked hard to make the most of the authorities, resources, and support that USCYBERCOM has received since its elevation to a unified Combatant Command in 2018. We optimized our force and operations to contest adversaries working to gain strategic advantage in and through cyberspace below the level of armed conflict. Recent events have shown how quickly new technologies can change the dynamics in cyberspace and also how rapidly competition can escalate into conflict. USCYBERCOM must be ready, which means added expectations for our force and capacity. I will explain in more detail what we are doing to address this challenge.

(U) WHO WE ARE

(U) The Cyber Mission Force (CMF) is the premier cyberspace force. Each of the Armed Services contributes service members to the CMF and they are the key to its success. Each one of the Service Cyber Component Commanders also serve as Joint Force Headquarters-Cyber Commanders reporting to the Commander of USCYBERCOM. Additionally, the command

works closely with Coast Guard Cyber Command within the Department of Homeland Security. Finally, it is important to note our DoD-wide 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).

(U) The National Security Agency (NSA) is our closest partner; our roles, missions, and responsibilities of USCYBERCOM complement those of the NSA, and vice versa. In 2022, the Secretary of Defense and Director of National Intelligence sponsored a study of the dual-hat leadership arrangement under which I serve as both the Commander of USCYBERCOM and the Director of the NSA. The study concluded that protecting our national security would be more costly and less decisive if NSA and USCYBERCOM were led by two different leaders, and that the dual-hat arrangement produces better outcomes for the nation. The Secretary of Defense, the Director of National Intelligence, and the Chairman of the Joint Chiefs of Staff subsequently determined to maintain the arrangement and we are now focused on ensuring an enduring and sustainable dual-hat arrangement.

(U) Our service members and civilians are aligned to the *National Defense Strategy.* We foster Integrated Deterrence through campaigning and building enduring advantage across the force by reviewing force generation, accelerating needed technology, and investing in our people. Our Code is "we win with people." USCYBERCOM personnel come to work every day to counter highly capable and determined adversaries who seek to harm the United States and its allies above and below the threshold of armed conflict. We strengthen warfighting advantage so we are prepared for conflict; strategic advantage below armed conflict, and decision advantage for policymakers and military commanders in strategic competition. We amplify the impact of Federal, military, foreign, and private sector partner activities and synergize how our nation applies all instruments of national power against adversaries.

(U) USCYBERCOM executes four assigned missions. We defend the nation from malicious cyberspace actors who threaten critical infrastructure and democratic processes. We defend Department of Defense Information Networks (DoDIN) to ensure mission advantage for the DoD. We integrate options and capabilities into Combatant Command campaigns and plans,

posturing to support the Joint Force across the conflict spectrum. And, we increase DoD cyber effectiveness through collaboration with allies and partners.

(U) SHIFTING THREATS

(U) The United States and our allies face sophisticated cyber threats from both state and non-state actors. Malicious cyber actors are difficult to observe and attribute. The People's Republic of China (PRC) and the Russia Federation have integrated cyber attack capabilities into military planning and operations to gain advantage during a crisis or conflict. In addition, Beijing, Moscow, and Tehran increasingly use social media and state-sponsored disinformation sites, both overt and covert, to shape narratives and sow confusion. We are particularly concerned with adversaries probing and exploiting our military and intelligence networks, compromising the U.S. defense industrial base networks in order to steal weapon system technology and accessing or attempting to compromise U.S. critical infrastructure. Additionally, our adversaries are targeting social media to coerce our personnel and monitor troop movements of U.S. forces.

(U) People's Republic of China (PRC)

(U) The PRC is our pacing challenge. The PRC is the only competitor with the intent and, increasingly, the capacity, to reshape the international order. The PRC is our closest competitor in cyberspace and central to the global technology supply chain; it employs the world's largest cyberspace operations workforce and an even larger set of enablers in its defense, cybersecurity, and information technology industries.

(U) USCYBERCOM is laser focused on the strategic and operational challenge the PRC presents in cyberspace. We seek in particular to support USINDOPACOM deter conflict and defend its area of responsibility, and to give ADM Aquilino the tools he needs to perform his missions. Additionally, we work daily to counter PRC-based cyber threats to our homeland, allies, and partners. We are particularly focused on defending against the PRC's persistent access and pre-positioning for attack on U.S. critical infrastructure systems. We will do everything we

can to deter the PRC from using these accesses to attack the United States. Our Command understands the value our allies and partners bring and will continue to work closely with them to counter PRC strategic intent. We have prioritized deterring and countering aggression both in the USINDOPACOM area of responsibility and globally. Overseeing this effort is the China Outcomes Group (COG), a USCYBERCOM-NSA collaboration illustrative of the value of our dual-hat command relationship. The COG enhances intelligence insights, improves cybersecurity, and delivers operational outcomes in support of Joint Force commanders and for the nation.

(U) Russia Federation

(U) Russia is an acute threat to the free and open global system. Moscow violates international norms with its continuing aggression in Ukraine, threatening the peace and stability of Europe. Moscow's need for more weapons and munitions has Russia buying arms from Iran and the Democratic People's Republic of Korea (DPRK) in violation of international sanctions. Indeed, Russia is strengthening ties with the PRC, Iran, and the DPRK to bolster its defense and commercial complexes, and this growing alignment poses a major challenge to the United States and our partners.

(U) Russia's military and intelligence cyber forces are capable and persistent. Their focus on the conflict in Ukraine has diverted, but not ended, their worldwide intelligence and operational efforts in support of Moscow's foreign policy. Russian actors also attempt to divide Western allies and undermine them both abroad and internally. Moscow likely views the upcoming U.S. election as an opportunity for malign influence and has previously targeted elections in the United States and Europe. We assess they will most likely do so again in this year's elections.

(U) In collaboration and coordination with USEUCOM, USCYBERCOM works with allies and partners to support Ukraine's independence and the success of its resistance to the Russian invasion. USCYBERCOM has collaborated with military and civilian partners since the crisis began in order to strengthen the DoDIN's security and defenses, enhance the resilience of

our NATO Allies, and assure the defense of our critical infrastructure, especially our nuclear command and control.

(U) Islamic Republic of Iran

(U) Iran's growing expertise and willingness to conduct malicious cyber operations make it a threat to the security of U.S. and allied networks. Iranian actors aggressively collect intelligence via the cyber domain, and back Tehran's objectives through cyber attacks, cyber-enabled propaganda, and regime control of domestic Internet access. We assess Iran particularly seeks to increase operations and targeting of industrial control systems to disrupt critical infrastructure.

(U) USCYBERCOM supports USCENTCOM in its work to deny and deter Iran. In addition, from the outset of the Israel-Hamas war, USCYBERCOM has supported significant efforts to 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) Democratic People's Republic of Korea (DPRK)

(U) The DPRK maintains increasingly capable cyber forces comprising both a growing cyber force within its borders and DPRK information technology workers living abroad. Pyongyang's use of cyberspace to collect intelligence, circumvent sanctions, and generate illicit revenue through cryptocurrency exploitation likely supports the regime's nuclear and ballistic missile programs, affecting regional and global security.

(U) Much as with Iran, USCYBERCOM works in alignment with USINDOPACOM's regional objectives of deterring war on the Peninsula and impairing the DPRK's ability to violate sanctions. In addition, the Command is working in support of national security objectives wherever DPRK cyber actors are seeking to counter allied global security interests.

(U) Non-State Actors

(U) Non-state actors remain a threat in cyberspace. Cyber criminals, some operating from Russia and with ties to Russian military and intelligence services, continue to find new victims in the United States and globally. USCYBERCOM and the NSA enable efforts by the Department of the Treasury, the Federal Bureau of Investigation (FBI) and other partners to disrupt ransomware, cryptocurrency theft, and other criminal activities. 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, and with allies and partners, to disrupt propaganda and mobilization online as well as to provide critical intelligence.

(U) Technology Change

(U) Technologies change rapidly, with the private sector driving many innovations. Automation, autonomy, and artificial intelligence proceed apace, boosting collection, detection, exploitation, maneuver, and command and control at ever greater speed and scale. Our allies, partners, and adversaries are all tracking and propelling this progress. For example, PRC investments in AI, cloud computing, 5G, and related technologies, coupled with the PRC's smart cities initiatives and extensive industrial base, guide its development and deployment of big data and AI for strategic advantage. Finally, we project that both the PRC and Russia will use artificial intelligence to develop autonomous cyber weapon systems to optimize offensive cyber operations.

(U) USCYBERCOM IN 2023

(U) USCYBERCOM's overarching responsibility is to defend the nation in and through the global and interconnected domain of cyberspace. Over the last two years we expanded our "Set the Theater" efforts to defend military systems and the data that they convey and store, which in turn provide warning, situational awareness, and synchronization and sustainment for

our fellow Combatant Commands in their respective geographic and functional areas of responsibility. In addition, we now work more intensively across the Joint Force and with a variety of partners to secure networks and the critical infrastructure that enable national security – what we call "Setting the Globe." Every Combatant Command operational plan across the Department assumes that our leaders and commanders can communicate orders and data securely. It is our job to ensure that foreign adversaries cannot impair that connectivity or decision-makers' trust in its security.

(U) The Cyber National Mission Force conducts missions to counter malicious cyberspace activities, supporting all aspects of our defend-the-nation mission set. CNMF personnel have deployed 22 times to 17 countries in partner-enabled, hunt forward operations that constrained adversary freedom of maneuver, supported our partners' efforts to increase cyber defenses, and generated important insights for our defense. And for the first time in the history of the Command there were active hunt forward operations occurring simultaneously in all Geographic Command AORs. These missions led to public releases of more than 90 malware samples for analysis by the nation's cybersecurity community. Such disclosures can make billions of Internet users around the world safer on-line, and frustrate the military and intelligence operations of authoritarian regimes.

(U) Enhancing the security of government, private sector, and critical infrastructure systems grows ever more imperative. Foreign adversaries continuously update how they operate, and frequently work through American-owned networks and devices. USCYBERCOM works in partnership with the Military Departments Counterintelligence organizations, the FBI-led National Counterintelligence Task Force, and DHS's Cybersecurity and Infrastructure Security Agency (CISA), sharing actionable intelligence that helps counter adversary activities, making them more expensive and less consequential. Consistent with Congressional support, USCYBERCOM is sharing information with industry to help bolster their ability to defend themselves against exploitation by malicious cyber actors, and to share more broadly the insights that both our industry partners and we gain from our collaboration. Our UNDERADVISEMENT program, a voluntary collaboration with dozens of private partners, links cybersecurity expertise across industry and government. It has led to dozens of operational successes to impose cost on

our adversaries, and enabled network owners to eradicate the threats from their systems. Due to the foresight of Congress, USCYBERCOM has enhanced authority to share information with private sector information technology and cybersecurity entities, enabling industry to defend itself better.

(U) USCYBERCOM and NSA are working with partners to counter foreign influence or interference in our upcoming elections. The prospect of undermining our democratic processes is too tempting for some foreign regimes and actors. The combined USCYBERCOM-NSA Elections Security Group (ESG) began working well before the start of the primary season to coordinate cybersecurity, intelligence, and operations, to better enable domestic partners to defend electoral processes. We are committed to supporting the interagency effort to ensure election contests across our states and territories proceed from caucuses to certifications without effective foreign influence. Let me assure you that our mission focus is foreign actors overseas. We shall work with scrupulous regard for the privacy and civil liberties of U.S. persons and in an objective, non-partisan manner as we have for the past six years.

(U) USCYBERCOM IN 2024

(U) USCYBERCOM campaigns in and through cyberspace to support national strategic goals in competition and set conditions for the Joint Force to deter and prevail in crisis and armed conflict. In 2024, we will create advantage for the warfighter, the Department, our partners, and the nation through enhancing readiness, implementing Service-like authorities, and advancing mission partnerships. Sustaining cyberspace operations at-scale against determined and capable adversaries was a requirement not fully projected when the Department established USCYBERCOM in 2010. We needed and received additional authorities and resources for this effort from 2018 onward. The foundation has been set, but now we must build on it.

(U) We have undertaken an initiative we call “CYBERCOM 2.0” to develop a bold set of options to present to the Secretary of Defense on the future of USCYBERCOM and DoD cyber forces. To maximize capacity, capability, and agility, we are addressing readiness and future force generation. Provisions on readiness and force generation in recent National Defense

Authorization Acts provide an opportunity for the Department to define the next decade of growth, impact, and warfighting outcomes by modernizing the cyber force, enshrine mechanisms for services/secretary-like oversight, and shape the future of USCYBERCOM.

(U) The Enhanced Budgetary Control (EBC) authority granted by Congress is transformational for the Command. When fully implemented with our FY24 appropriation to USCYBERCOM, it entrusts more than $2 billion in DoD budget authorities to USCYBERCOM, and streamlines how we engage the Department's processes. EBC is already paying dividends in the form of tighter alignments between authorities, responsibility, and accountability in cyberspace operations. Greater accountability, in turn, facilitates faster development and fielding of capabilities.

(U) Agile acquisition is crucial to creating advantage for our commanders, component elements, and operators. The most important effort in this regard is our Joint Cyber Warfighting Architecture (JCWA), an integrated system of systems with associated capabilities that facilitate the full-spectrum of cyberspace missions and foster overmatch against evolving, sophisticated, and motivated adversaries. JCWA is accelerating tool development and data flows within and across the Command and mission partners. In 2024, the Command will partner with the Services and DARPA (among others) to ensure our acquisition strategies can achieve agility, scale, and precision at cyber-relevant speed.

(U) USCYBERCOM recently received the JCWA systems engineering and integration (SE&I) authority from the Office of the Under-Secretary of Defense for Acquisitions & Sustainment (OUSD (A&S)). The SE&I authority will allow USCYBERCOM to define the interoperability standards between the subcomponents of JCWA, currently managed by the Services. In addition, OUSD (A&S) is working with USCYBERCOM to establish Program Executive Office (PEO) JCWA and provide milestone decision authority/decision authority at the appropriate point as the PEO grows in size and capability.

(U) All of these efforts begin with people. We must hire and retain the right talent and keep our personnel ready to meet the challenges of competition and conflict in and through

cyberspace and the information environment. 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 is now able to ingest data directly from the Defense Readiness and Reporting System without manual input. USCYBERCOM's authorities as Joint Cyberspace Trainer will enable Joint training standards across the entire Department, boosting its ability to defend networks while enabling CMF teams to focus on hunting and contesting foreign adversaries. Additionally, over the past year, we have worked to fill our civilian billets, driving down security and personnel processing times by 25 percent and accelerating hiring actions to fill more than 250 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. We have made job offers to key experts and look forward to hiring more in 2024. Indeed, we are maximizing use of DoD Cyber Excepted Service authority to streamline civilian hiring and offer competitive employment incentives.

(U) This year will mark the first year in which the Department of the Army is acting as the Combatant Command Support Agent (CCSA) for USCYBERCOM. The Army's military and civilian leaders have been superb in managing this transition and making sure our civilians experience this as a seamless and transparent process. USCYBERCOM is also 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 engage National Guard units on State Active Duty and State Partnership Program engagements.

(U) Strong partnerships with government, industry, academia, and foreign colleagues amplify our effectiveness and create advantages in turn for our partners. 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 will guide efforts with partners such as Australia, Japan, and South Korea to counter and contest foreign adversaries.

(U) Our Academic Engagement Network (AEN) of more than 120 institutions is unlocking new partnerships and bringing fresh ideas to our mission challenges. The AEN is able to tap into a broad knowledge base to encourage in-depth analysis in areas where we lack expertise. Through Cooperative Research and Development Agreements (CRADAs) and Education Partnership Agreements (EPAs), USCYBERCOM is formalizing and enhancing its AEN relationships. USCYBERCOM signed its first EPA with Norwich University in November 2023, and USCYBERCOM signed an EPA and a CRADA with the University of Missouri - Kansas City (UMKC) this January.

(U) Finally, in an environment transformed by Artificial Intelligence and big data, operational and strategic advantage will accrue to the side that achieves and sustains superiority in collecting and ingesting data, building models and algorithms, and deploying and updating them at-speed and scale—while also denying the same to adversaries. We are focused on ensuring our data and analytic infrastructures deliver advantage over adversaries, and that those systems have deep resilience that enables them to function even under attack. The FY23 National Defense Authorization Act called on DoD and USCYBERCOM to develop a five-year AI Roadmap for adoption of AI for cyberspace operations. Finalized in September 2023, this AI roadmap enables DoD and USCYBERCOM to accelerate adoption and scale capabilities across the Joint Force. We have employed forms of AI for years now in various aspects of our work, and we know that people, data, organization, and infrastructure are critical elements to future success. Our collaboration with more than a dozen partner organizations has fostered a community to drive Roadmap implementation in three main areas: delivering AI capabilities for all cyberspace mission sets; countering AI threats and exploiting emerging opportunities; and enabling AI adoption. We recognize the need to employ multiple innovation strategies to achieve speed, agility, and scale in operations, capability development, data sharing, and procurement.

(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 work every day against capable

and determined cyber actors, many of them serving adversary military and intelligence services. Our operational experience reinforces the importance of campaigning globally in and through cyberspace across the conditions of competition, crisis, and armed conflict. The Command now has ample authorities to plan, program, budget, and execute the Program Objective Memorandum; control budgets; and set and validate requirements. It has a mandate to partner with the services to organize, train, and equip the force. Fully executing the tasks assigned to us with the significant new resources and authorities Congress and the Executive Branch have provided is bringing us closer to operating with the speed, scale, agility, and precision that the cyber strategic environment demands. We must realize our full potential in creating advantage. We will collaborate, innovate, and accelerate for future success.

(U) The men and women at USCYBERCOM are grateful for the support this Committee has given to our Command. Our service members and civilians look forward to demonstrating how well they can manage their responsibilities and accomplish their missions to strengthen our nation's security. With continued strong partnership with Congress, I know we will succeed. Thank you. I look forward to your questions.