S. HRG. 119–75, PT. 8

DEPARTMENT OF DEFENSE AUTHORIZATION REQUEST FOR APPROPRIATIONS FOR FISCAL YEAR 2026 AND THE FUTURE YEARS DEFENSE PROGRAM

HEARING

BEFORE THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION
ON

S. 2296

TO AUTHORIZE APPROPRIATIONS FOR FISCAL YEAR 2026 FOR MILITARY ACTIVITIES OF THE DEPARTMENT OF DEFENSE AND FOR MILITARY CONSTRUCTION, TO PRESCRIBE MILITARY PERSONNEL STRENGTHS FOR SUCH FISCAL YEAR, AND FOR OTHER PURPOSES

PART 8
CYBERSECURITY

APRIL 9, 2025

Printed for the use of the Committee on Armed Services

U.S. GOVERNMENT PUBLISHING OFFICE
61–986 PDF WASHINGTON : 2025

DEPARTMENT OF DEFENSE AUTHORIZATION REQUEST FOR APPROPRIATIONS FOR FISCAL YEAR 2026 AND THE FUTURE YEARS DEFENSE PROGRAM—Part 8 CYBERSECURITY

S. HRG. 119–75, PT. 8

DEPARTMENT OF DEFENSE AUTHORIZATION REQUEST FOR APPROPRIATIONS FOR FISCAL YEAR 2026 AND THE FUTURE YEARS DEFENSE PROGRAM

HEARING

BEFORE THE

OF THE

COMMITTEE ON ARMED SERVICES UNITED STATES SENATE

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

ON

S. 2296

TO AUTHORIZE APPROPRIATIONS FOR FISCAL YEAR 2026 FOR MILITARY ACTIVITIES OF THE DEPARTMENT OF DEFENSE AND FOR MILITARY CONSTRUCTION, TO PRESCRIBE MILITARY PERSONNEL STRENGTHS FOR SUCH FISCAL YEAR, AND FOR OTHER PURPOSES

PART 8
CYBERSECURITY

APRIL 9, 2025

Printed for the use of the Committee on Armed Services

Available via: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
61–986 PDF WASHINGTON : 2025

COMMITTEE ON ARMED SERVICES

ROGER F. WICKER, Mississippi, *Chairman*

DEB FISCHER, Nebraska
TOM COTTON, Arkansas
MIKE ROUNDS, South Dakota
JONI K. ERNST, Iowa
DAN SULLIVAN, Alaska
KEVIN CRAMER, North Dakota
RICK SCOTT, Florida
TOMMY TUBERVILLE, Alabama
MARKWAYNE MULLIN, Oklahoma
TED BUDD, North Carolina
ERIC SCHMITT, Missouri
JIM BANKS, Indiana
TIM SHEEHY, Montana

JACK REED, Rhode Island
JEANNE SHAHEEN, New Hampshire
KIRSTEN E. GILLIBRAND, New York
RICHARD BLUMENTHAL, Connecticut
MAZIE K. HIRONO, Hawaii
TIM KAINE, Virginia
ANGUS S. KING, Jr., Maine
ELIZABETH WARREN, Massachusetts
GARY C. PETERS, Michigan
TAMMY DUCKWORTH, Illinois
JACKY ROSEN, Nevada
MARK KELLY, Arizona
ELISSA SLOTKIN, Michigan

John P. Keast, *Staff Director*
Elizabeth L. King, *Minority Staff Director*

Subcommittee on Cybersecurity

MIKE ROUNDS, South Dakota, *Chairman*

TOM COTTON, Arkansas
JONI ERNST, Iowa
TED BUDD, North Carolina
ERIC SCHMITT, Missouri

JACKY ROSEN, Nevada
KIRSTEN E. GILLIBRAND, New York
GARY C. PETERS, Michigan
ELISSA SLOTKIN, Michigan

CONTENTS

APRIL 9, 2025

MEMBERS STATEMENTS

WITNESS STATEMENTS

DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2026 AND THE FUTURE YEARS DEFENSE PROGRAM

WEDNESDAY, APRIL 9, 2025

UNITED STATES SENATE,
SUBCOMMITTEE ON CYBERSECURITY,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

UNITED STATES CYBER COMMAND

The Committee met, pursuant to notice, at 3:40 p.m. in room SD-G50, Dirksen Senate Office Building, Senator Mike Rounds (Chairman of the Subcommittee) presiding.

Committee Members Present: Senators Rounds, Rosen, King, and Reed.

OPENING STATEMENT OF SENATOR MIKE ROUNDS

Senator ROUNDS. Good afternoon. I'd like to express my gratitude to Lieutenant General Hartman for his attendance at today's hearing.

Before I proceed any further, I want to acknowledge the incredible momentum set by General Haugh and the strategic transformation needed to meet the evolving threats of today and the emerging challenges of tomorrow in cyberspace. General Haugh was a strong leader with a deep knowledge of the art and science of cyber warfare, hard earned over three decades of service to our country.

Men and women capable of leading the National Security Agency and the United States Cyber Command are in short supply. Such leaders require years of experience to develop with deliberate and dedicated career focus. To put it more directly, we do not have enough of these types of leaders, and a loss of any one of them without strong justification is disappointing. The departure of General Haugh is a loss for our Nation, but will be a tremendous gain for any private or public entity where he decides to lend his expertise and leadership. I wish him Godspeed.

That said, as our adversaries watch this hearing, it will be clear, that no matter the scenario, our cyber mission forces are ready. Lieutenant General Hartman's presence is more than just an annual congressional activity. His presence is more than just a general annual congressional activity. It shows the strength and resiliency of the cyber mission force. It is a testament to how much this command has matured since its inception in 2009, and the steadfast nature of our military, civilian and uniformed, to step up and fight when the Nation needs them.

It also reflects the absolute importance of the dual hat arrangement, in the face of unexpected change there remains tight integration of cyber and intelligence operations, thanks to alignment under a single leader. Such an arrangement remains paramount in future decisions of General Haugh's formal successor.

I have had the pleasure of working with Lieutenant General Hartman in his prior role as Deputy Commander of the United States Cyber Command, and I am confident in his ability to lead these organizations through this transition, maintaining the combat capability of a force that operates in an environment of constant change. He is one of the few, with a strong understanding of this domain, built over decades of experience.

The importance of the cyber domain cannot be overstated. Our adversaries understand the dynamic and permeable nature of cyberspace and have clearly demonstrated their intent to exploit it to their advantage. General Hartman, as we discussed in detail during our closed session, the threats our Nation faces in the cyber domain have only intensified since we last convened for an update from United States Cyber Command (CYBERCOM) a year ago.

The detection of additional Chinese advanced persistent threat groups throughout the past year has reinforced both the determination of our adversaries to own this domain, and their technical capability to do so. With the release of the Chinese generative artificial intelligence, large language model or DeepSeek-R1, earlier this year, competitive advantage will now be measured in weeks and months, not years. Our cyber mission force must be ready with training, technology, and operational structure to deter and defend against this new reality.

I have been encouraged by the work the command has conducted on CYBERCOM 2.0 in collaboration with the services and the Assistant Secretary of Defense for cyber policy. I want to hear what policy changes are needed to realize the vision behind this effort. While I understand the implementation plan has not been delivered to Congress, our adversaries are not waiting for our process to conclude.

I look forward to hearing more from you about the efforts underway to implement CYBERCOM 2.0 and how you intend to make sure the force is maturing, to conduct persistent engagement in this competitive environment.

I will now recognize Ranking Member Reed, from the full Committee, at Senator Rosen's request, for opening remarks.

STATEMENT OF SENATOR JACK REED

Senator REED. Thank you very much, Mr. Chairman, and thank you Senator Rosen. I just want to take a moment to recognize General Haugh for his 35 years of dedicated service to this country and to the United States Air Force.

His sudden and inexplicable firing is disrespectful to his service, but also disrespectful to every military member in or out of uniform, and an indication that their service and sacrifice is in no way respected by this Administration. The callous nature of the decision, the result of a meeting with a partisan conspiracy theorist, not on any kind of informed or experienced judgment, puts our security at grave risk and cannot be tolerated or continued.

We salute a dedicated American for his service and sacrifice and his family for standing with him and wish him well. Thank you, Mr. Chairman.

Senator ROUNDS. Ranking Member Rosen.

STATEMENT OF SENATOR JACKY ROSEN

Senator ROSEN. Thank you, Chair Rounds, and thank you Ranking Member Reed. Of course, this is such an important hearing, and I appreciate General Hartman, our meetings that we had yesterday and your team, all of your service, your commitment to the mission and on the success, because that means that we're all kept safe.

You're also here on very short notice, as we've all been talking about, and we appreciate that as well, and so, I look forward to continuing our conversations and our continued partnership to ensure that success.

Like my colleagues, I want to begin by addressing a matter of significant concern, the sudden and inexplicable firing of General Haugh, a trusted and dedicated Air Force officer for over 34 years, a true patriot. His abrupt and unjustified removal was conducted in the dead of night, with absolutely no consultation with Congress, the full committee, or this Subcommittee.

According to press reports, it was at the request of a private individual outside of the government, outside the chain of command, who has a long record of pedaling in vicious conspiracy theories. This action compromises CYBERCOM and the National Security Agency (NSA) ability to keep Americans safe.

United States faces major cyber threats from foreign adversaries, China, Russia, Iran, near daily cyber-attacks and our critical infrastructure. At the same time, we are engaged in ongoing operations against multiple threats across the globe, from Russian aggression against Ukraine to Iranian backed proxies in the Middle East and North Africa.

Given the dangers facing the United States and our troops, it is inexplicable and unconscionable that the President would, at the mere request of an online provocateur, remove the leader of CYBERCOM, completely without cause and in doing so, risk undermining vital intelligence operations.

Moreover, General Haugh has been a trusted leader. His experience and expertise have been crucial in guiding and shaping the efforts of U.S. Cyber Command and our overall national defense posture. At a time when our adversaries are constantly evolving their cyber capabilities, whether it's from State actors like Russia, China, Iran, or North Korea, or non-State actors with nefarious intent, leadership continuity and clear vision are more critical than ever.

Cybersecurity and cyber operations are not and cannot be a partisan issue. It is a national security imperative, and the threat environment as we all know, continues to intensify every single day. We must maintain experienced leadership to counter the ever-evolving cyber challenges facing our country. As Members of this

Committee and the full committee, we must demand clarity from the administration about the rationale for this decision, and we must not rest until we have answers and accountability from both President Trump and Secretary Hegseth.

This afternoon though, our focus will be on our Nation's cyber capabilities and how Congress can help support the critical work that CYBERCOM personnel do every single day. I might say 24 hours a day, 24–7, 365.

I look forward to hearing from General Hartman and to discussing how we can meet our Nation's challenge. Today, in the future and over the course of this congress, again, I know how much General Hartman you are invested in the mission of CYBERCOM, how much you know about it, your experience, your expertise and how invested you are in the ongoing success in combating cyber threats going forward. I do look forward to working with you on that. So, thank you, Mr. Chairman.

Senator ROUNDS. Thank you, Ranking Member Rosen, and with that, Lieutenant General Hartman, welcome. Thank you for your service. We thank your family as well for their sacrifice, and there's a lot of things that you literally don't get an opportunity to share with the American public because of the type of responsibilities that you have. But today, you have an opportunity to share with the American people and with this committee a little bit about what you are doing. We welcome your opening remarks at this time, sir.

STATEMENT OF LIEUTENANT GENERAL WILLIAM J. HARTMAN, USA ACTING COMMANDER, UNITED STATES CYBER COMMAND/ ACTING DIRECTOR, NATIONAL SECURITY AGENCY/ ACTING CHIEF, CENTRAL SECURITY SERVICE

Lieutenant General HARTMAN. Good afternoon. Chairman Rounds Ranking Member Rosen, thank you for your unwavering support and for the honor of representing U.S. Cyber Command today.

I'm here to discuss the evolving strategic landscape and our approach as we look forward to 2026. CYBERCOM's mission is straightforward: We defend the Nation from cyber threats, we protect the Department of Defense's Networks, and we support the joint force. We are dedicated to ensuring the Department's mission advantage, and providing options across the conflict continuum to the President, the Secretary of Defense, and the American people.

Achieving our assigned objectives in the mission set forth by the President of "Peace through strength", requires a force equipped with a strong warrior ethos and the lethality necessary to meet our national objectives.

Deterrence is essential to our strategy. In cyberspace, we're focused on maintaining a credible capability that dissuades adversaries from targeting our critical infrastructure. Cyberspace is a rapidly evolving domain influenced by technological advancements, which necessitates a close partnership with industry. As the environment changes, CYBERCOM will adapt by swiftly developing and deploying new capabilities. Our commitment is to lead from the front, staying ahead of threats, through a proactive and agile approach.

Our people are our greatest asset, capturing our ethos, we win with people. The dedicated professionals of CYBERCOM are at the forefront, defending networks, encountering threats every day. Their innovation and perseverance are essential to maintaining our Nation's advantage in cyberspace.

But we're not alone in the fight. Our allies and partners are crucial components of our collective defense. Key collaborations like our partnership with the National Security Agency, enhance our Nation's security by creating a unified effort that surpasses the capabilities of our adversaries.

Moving forward in 2026, our focus is not only on maintaining readiness, but also elevating the level of mastery within our cyber forces. Our initiative, CYBERCOM 2.0 seeks to overmatch our adversary's quantity with the quality of our people, capabilities, and operations. Modernizing our force design and rapidly integrating new technologies, are vital components of our strategy here. Partnership with industry and academia become indispensable, enabling us to stay at the forefront of cybersecurity advancements.

Our adversaries are persistent and they are sophisticated. State sponsored cyber actors from China, Iran, North Korea, and Russia, pose significant threats to our critical infrastructure and military systems. China is the most persistent threat while Russia has gained significant capabilities through their ongoing operations.

To counter these threats, CYBERCOM develops robust deterrent strategies, ensuring that any attempt to undermine our security will face an overwhelming response. An essential part of our future strategy includes the accelerated integration of artificial intelligence. Artificial intelligence offers unparalleled speed and precision in cyberspace operations, making it a key enabler for anticipating and countering emerging threats.

By expanding Artificial Intelligence (AI) across our operations, we will strengthen our deterrence posture and maintain superiority in the cyber domain. True excellence in AI requires a world class workforce. Through initiatives like CYBERCOM 2.0, CYBERCOM will continue to collaborate with the Department to develop, pilot, and implement new tools and opportunities to invest in our workforce. A world class workforce requires world class training, facilities, and capabilities to excel and thrive. With the support and assistance, we received from the Department and from Congress, CYBERCOM is well positioned to achieve these world class results.

Our work is far from finished, but with your continued partnership, I'm confident we'll succeed in defending our Nation. CYBERCOM is prepared to rise to the challenge, outpacing our adversaries, securing our interests, and protecting our future.

Thank you, and I look forward to answering any questions you may have.

[The prepared statement of Lieutenant General Hartman follows:]

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.

Senator Rounds. Thank you, General Hartman. I'll begin. In the wake of the various persistent cyber threats originating from the People's Republic of China over the last 2 years, it is my firm conclusion that the importance of the dual hat is as important today as it has ever been.

Given these events, how has the dual hat arrangement between USCYBERCOM and NSA evolved to address the emerging threats from our adversaries?

Lieutenant General HARTMAN. Senator, thank you for your question. The relationship between CYBERCOM and NSA continues to evolve so that we really achieve two key objectives. The first is that we see and understand what our adversary is doing. The second piece of that is that, we enable CYBERCOM or other elements of the U.S. Government in order to operate, in order to defend our critical infrastructure, our key networks and the Department of Defense Information Network.

The ability for us to execute those operations clearly, understanding that we have to act, but that we also have to protect things like intelligent sources and methods, is fundamentally important to the dual hat. From my standpoint—and Senator, I've been sitting on the campus of the National Security Agency in CYBERCOM for most of the last 15 years, I've continued to see this partnership evolve, and our ability to execute increasingly more precise operations is fundamentally because the dual hat allows me, in my current capacity, to move with the speed and agility of unity of effort that is required, but it also forces leaders across the organization to collaborate, to do the hard work and to provide the best options for the national security of the country.

That's what I believe is the importance of the dual hat, and that is really where I believe we've evolved to.

Senator ROUNDS. Recognizing that this is an open setting and we can't get into specifics. I think another item, not only the dual hat, has been successful, but also the NSPM 13 [National Security Presidential Memorandum 13], which was incorporated under President Trump in his first term, I believe, has been very successful in the process.

The determining of when you can do your offensive cyber operations in an efficient manner, and making sure that all parties involved are appropriately apprised, but there is a decision process in place. Can you talk a little bit about the successes in terms of just the magnitude of the successes that you have seen achieved since the creation of the National Security Policy Memorandum 13 by President Trump in his first term?

Lieutenant General HARTMAN. Thank you, Senator Rounds for the question. NSPM 13 is a repeatable, sustainable, agile process that is recognized across the Department of Defense and across the interagency that allows us to move at the speed and agility that's required, based on our intelligence, based on operational requirements, and it has increased our ability to execute cyber operations tenfold.

Senator ROUNDS. Excellent. Thank you. This is just to give the American public some sense of what happens when you do the dual hat, and you also have the ability to make the decisions and to move quickly, how quickly we can actually accommodate our need for offensive cyber operations. Thank you for that information.

Lieutenant General Hartman, in the commands testimony last year, General Haugh previewed the CYBERCOM 2.0 initiative, to focus on delivering a bold step forward in the future of the Cyber Mission Force. What is the status of this effort and what are the major recommendations of this plan?

Lieutenant General HARTMAN. Chairman Rounds, thanks for the question. As you're well aware, one of the impetuses for

CYBERCOM 2.0 was Section 1533 of last year's National Defense Authorization Act. Based on that, we put together a planning team and really studied hundreds of different references over the last year, and studied different force presentation models. We briefed the recommendations of CYBER COM 2.0 to the last administration and the Secretary of Defense approved it. We briefed this to the new Secretary of Defense who asked us to work the implementation strategy that we were previously working on a 6-month timeline down to 45 days.

So, we brought an operational planning team together, or really what we called a cross-functional team. Over the last 45 days, we've submitted a series of recommendations that we have concurrence, generally from across the services and across the Department, which honestly is pretty extraordinary in a 45-day time period, for us to get that level of consensus.

Those recommendations are really built around how do we improve talent management in the force? How do we improve advanced training in the force? and how do we improve our ability to innovate and bring new capabilities to the force at the scale and speed that we need to compete with our adversaries there.

That seems relatively simple. It's about 80 pages; we've delivered it to the Department. The Department is going through a very reasonable process and we're pending the results of that feedback from the Department chairman.

Senator ROUNDS. Thank you General. Ranking Member Rosen.

Senator ROSEN. Well, thank you. I want to talk a little bit maybe about policy challenges. So, as we continue to evolve and develop our cyber capabilities to address the emerging threats, it's clear that there's a number of challenges, both within the Department of Defense and across agencies that can impede everybody's progress.

I'd like to ask you about these obstacles and how they impact CYBERCOM's efforts to stay ahead of the growing cyber threat landscape. So, we know that you have many challenges, but based on CYBERCOM's plan for development, could you speak to some of the key policy obstacles that remain challenges for your operations, both within the Department of Defense and in the broader interagency context?

Lieutenant General HARTMAN. Senator Rosen, thanks for the question. First, I just want to highlight that I think we have made significant progress. You know, one of the things we have discussed previously is the ability for us to support critical infrastructure that is off Department of Defense Information Network (DODIN), but critical to the Department's mission.

We do appreciate the support from Congress in giving us the Federal labs authority that has allowed us to execute cooperative research agreements. I know that we've talked about Guam being a key component of this, and, you know, I, I'm happy to report that we have executed six different craters over the last 6 months with a number of very important critical infrastructure organizations in Guam. Our assessment is we have reduced the threat that those organizations face by about 25 percent.

That has been really key for us. We continue to work to better integrate the Reserve component into our operations to help secure critical infrastructure. It is an area where we think we need both an improvement from a policy standpoint, but we also need improvement from an appropriation standpoint, so we're able to better leverage the Reserve component force in order to support some of these critical mission sets.

Senator ROSEN. So, could you elaborate a little further maybe, with the primary sticking points what would hinder that coordination effectiveness, expansion of our cyber capabilities? Are you taking some steps there or how can we help as we begin to think about what those policy and appropriations needs might be?

Lieutenant General HARTMAN. Senator Rosen, thanks for the question. I think on the defense of critical infrastructure, there continues to be a key role that a number of different organizations will take. I don't believe the Department will necessarily be the lead, but you know, there are recommendations that we will bring to the committee to how we might better work with organizations like the Department of Homeland Security, certainly organizations like the National Guard Bureau and we do believe that there are some policy recommendations that will work through the process that will be beneficial.

I didn't talk about the United States Coast Guard. The United States Coast Guard has been a key partnership over the last 12 months. We have signed a memorandum of understanding with the Coast Guard. So, as a Coast Guard executes operations under the Department of Homeland Security (DHS) authorities, we do have the ability to support their operations, in a case where they have an authority, but they don't have the capacity. Certainly, as we look at the security of port facilities, critical infrastructure that supports port facilities, that is what we think is a very important MOU [Memorandum of Understanding].

At the same time, if we have a CYBERCOM mission, we're operating on a facility that is specifically suited to the expertise the Coast Guard brings, they also have the ability to reinforce our operations. I do think we've made progress. I think there are additional policy recommendations. Senator, I look forward to working with the committee in order to provide those recommendations.

Senator ROSEN. Thank you. I want to talk a little bit about cyber workforce, because you can't do any of this without maintaining a robust cyber workforce. Our defense posture depends on it, we have to be sure that they're capable, that they're equipped, that they're trained, like you're talking about, these are our challenges to constantly be training, working on the mission, because the threats are ever evolving. The cyber domain is incredibly dynamic and achieving mastery it's just crucial, and it isn't done overnight.

So what steps are you taking in CYBERCOM to make sure that we're keeping our personnel ahead of the curve? Talk to me about the workforce cuts and the hiring freeze and how that's impacting your ability to meet the mission.

Lieutenant General HARTMAN. Senator Rosen, thanks. First of all, I would like to highlight that over the last year, we've had a number of things that have significantly impacted how we're managing particularly our civilian workforce.

The first is the Cyber Excepted Service (CES). The ability to hire under CES has reduced the lag time by 45 percent, from over a year to less than 6 months now, in order to bring civilian personnel on board, that has been impactful. We went through a transition from what we call a Combatant Command Support Agency, from the Department of the Air Force to the Department of the Army. I'm in the army, but I'm not saying one is better than the other. But the transition, you know, did provide a little bit of friction as we work from one service to the other.

We transitioned to the army last June and that has improved sort of a repeatable process to bring the civilians on board. Then there have been things like the 4092 authorizations from Congress, that have been important and allowed us to hire really, really high-end talent. So, I think we are on a glide path.

The current hiring freeze has impacted our ability to bring new hires into the force. We'll continue to work with the Department on the way ahead for that. We have, however, not been impacted by any cuts. We have been able to go back to the Department and get an exemption.

It is important because, as I think you're aware, Senator, we're only a little over 50 percent man with our civilian force but It's because those authorizations have all come really in the last year and a half. So, we do think it's important to get the civilian hiring freeze moved, and we do think it's important to be able to rapidly bring talent into the force.

Senator ROSEN. Thank you.

Senator ROUNDS. General, I have just one other question. In early 2024, Congress received a briefing on the commands AI roadmap as required by the fiscal year 2023 National Defense Authorization Act. Given the release of the Chinese generative AI model, DeepSeek-R1, what steps has the command taken to accelerate delivery of the capabilities and milestones in this roadmap? What is needed to make certain that we will be successful in this acceleration?

Lieutenant General HARTMAN. Chairman Rounds, thanks so much for the question, and so over a year ago, we produced again, based on a congressional requirement, so thanks, our AI roadmap that laid out a plan for the next 5 years. Very close partnership with NSA, and their artificial intelligence experts. A little over a year ago, we decided that we had a really good plan from a staff standpoint, but where CYBERCOM could add value, was in operationalizing these capabilities.

So, we took the majority of the staff portion of that AI task force, and we moved it to the Cyber National Mission Force. We went out and hired some additional AI talent, really focused on 90-day pilot projects that we could evaluate, and if successful, we could scale across the force. If they weren't successful or didn't meet a need that we would then focus our efforts elsewhere.

Over the last 12 months, we have executed artificial intelligence pilots to secure the DODIN, right? This is at the edge of the DODIN network, this is across network devices and it's at our end points. It has been very successful, and it is where we're moving to in the future.

We have integrated large language models into our "hunt forward" kits. We have integrated large language models into our offensive capabilities. We have partnered very closely with DARPA

[Defense Advanced Research Projects Agency], under Project Constellation and continue to transition capabilities, mostly based on artificial intelligence to the force.

Additionally, Senator, we have and will continue to work with the Department on long-term resourcing that ensures we maintain advantage over China and any other adversary. I will say, we were all—paid close attention to, and we're alarmed by the DeepSeek model, right, But the United States of America builds the best software in the world, all right. We believe working with private industry, working across the government, that unique advantage in building the best software in the world, will allow us to stay ahead of the Chinese.

Senator ROUNDS. Thank you General. Ranking Member Rosen.

Senator ROSEN. Thank you. I want to build a little bit on Senator Round's AI question, because we look to the future of cybersecurity. How else do we need, besides artificial intelligence, how do we need to adapt our training and development pipeline to ensure that our human workforce achieves mastery in the cyber domain?

Additionally, with the increasing demands on our personnel and the nature of the cyber operations, how else can we perhaps leverage industry or commercial training opportunities to supplement the more specific on-net training that takes place in a classified environment?

Lieutenant General HARTMAN. Senator, thanks for the question. You know, we've talked about CYBERCOM 2.0 and one of the big ideas in CYBERCOM 2.0 is advanced training. right? Right now, CYBERCOM is very fortunate and the services have done a very good job in order to present a C2 [Command and Control] force. The first time in the history of the command over the last year, we've reached C2, which means manned 80 percent in the aggregate and trained it to 70 percent.

But as we look at things like artificial intelligence, and cloud computing, and data scientists, and other advanced capabilities, we do think that the model we've laid out in CYBERCOM 2.0 is really where we need to go. It's my role with service-like authorities and as a joint force trainer, to take servicemembers and civilians that are presented to us by the services, and take them from that basic level and make them masters, and that is masters in data science, that's masters in cloud computing, that's masters in artificial intelligence.

Then immediately take those lessons and feed them back, not only into the training base from the services, but also into our operational organization. That is really the best way that we think we can get after the training part of this. We are also working very closely with private industry, the creator authority that the committee has given us, also allows us to execute creators within private industry. We continue to work very closely with UARCs [University Affiliated Research Centers] and FFRDCs [Federally Funded Research and Development Centers], who provide us access to really high-end, really responsive talent, particularly as it relates to artificial intelligence and machine learning.

Senator ROUNDS. Thank you, and I do believe we have another Member that is just arriving, and I would simply ask Senator King, are you ready with questions?

Senator KING. I'm always ready.

Senator ROSEN. I was going to say I knew how he would answer that. He's always ready.

Senator ROUNDS. Senator King.

Senator KING. Thank you very much General for being here today. I take it my colleagues have talked, I'm sorry. I was at a hearing upstairs in the Intelligence Committee and it was an open hearing, so I can even tell you about it. But in any case, I understand that my colleagues have talked a lot about the firing of General Haugh and how unfortunate that was, so I don't need to plow that ground.

One of the issues that I'm principally concerned with in cyber, is that we have no deterrent. Our strategy in all of our other military and national security approaches is based upon deterrence, except in cyber, where we continually are attacked, as we were salt typhoon for example, going all the way back to Sony, nothing ever happens to the adversary. My belief is, that until we start to impose costs and they understand that there will be costs, these attacks are going to continue, they're cheap, and there's really no consequences.

If you're sitting in the Kremlin and somebody said, let's interfere with the next election in the United States, your answer would be, why not? It's not going to really cost us anything, and they don't respond, we're not in at any risk. Do you agree with me that we need to have a more stronger retaliatory capacity, No. 1, and demonstrate the will to use it? Otherwise, these attacks are simply going to continue.

Lieutenant General HARTMAN. Senator, thanks for your question. It's good to see you again.

Senator KING. Yes, sir.

Lieutenant General HARTMAN. So, Senator, we certainly agree that we need to continue to improve our capability in order to deter and respond to attacks. I will tell you that from our standpoint, there is certain activity that adversaries to include China, will always continue to conduct. We got to focus on the most credible capabilities to deter operations that significantly impact the national security.

Just like you, I am aware of salt typhoon and volt typhoon, and while we're certainly concerned about that, and we will certainly develop a broad range of options to deal with that, I will tell you that the fact that we are able to see and observe that activity, and we are able to work with industry partners in order to build defenses against that activity, is something that provides us some advantage vis-a-vis adversaries like the Chinese.

I assure you, we are dedicated to developing options in order to counter that. I would be more than happy to work with your staff in a different setting to provide you some details.

Senator KING. Well, I understand that you have capacity and you have capabilities. We demonstrated that in 2018 with the hunt forward, defend forward, that General Nakasone initiated. So, I understand we have the capacity. My problem is we don't have a doctrine. We don't have—a deterrence doesn't work unless the other side knows about it. Dr. Strangelove, why didn't you tell us about the doomsday machine? Well, the Premier like surprises.

A deterrent isn't a deterrent: It takes two things, three things, capacity-which we have, will-which we apparently don't have and knowledge of the adversary that—we have those two things, and that they're being held at risk.

So, I'm not questioning the capabilities. What I'm questioning is, here we are with salt typhoon, you know, two or three, 6 months ago nothing's happened, no response, no. You know, like I said, we haven't even responded to the Sony attack, and that was 10 or 15 years ago. There's never a price to be paid by our adversaries. Until we develop that theory, it seems to the concept of deterrence, and let them know that they're at risk, they're going to keep doing what they're doing.

I understand defending and working with our private sector partners, that's all good. But you can't patch your way out of this. There's got to be, I believe, a credible deterrent that the adversaries understand, that if they attack us in cyberspace, they will pay a price. It doesn't necessarily have to be in cyberspace. It may be some other kind of harm that puts them at risk.

But the point is, until we start to develop that doctrine and let our adversaries know, it's just going to keep happening.

Lieutenant General HARTMAN. So, Senator, I acknowledge your concern. Again, I look forward to working with the committee, with the Department and I do think we could provide you some more information in a closed session.

Senator KING. Well, I appreciate that. Thank you, Mr. Chairman.

Senator ROUNDS. Thank you, Senator King. I do have one last question for you, General and then I will allow Ranking Member Rosen a final question as well.

Last year, the Defense Science Board briefed Congress on the status of the Joint Cyber Warfighting Architecture or JCWA. How is this command addressing the Defense Science Board's concerns about excessive bureaucracy, and length the acquisition timelines, that prevent cutting edge cyber technologies from being integrated into the Joint Cyber Warfighting Architecture, before they become obsolete?

Lieutenant General HARTMAN. Chairman Rounds, thanks for your question. In the 2022 National Defense Authorization Act, CYBERCOM was given a number of things, we put it under the banner of service like authorities. One of those was acquisition authorities. The other piece was enhanced budget control.

Under those authorities, we have consolidated our efforts as it relates to JCWA, and we are fielding relevant, agile, and not obsolete capabilities, that are positioning us to execute our UCP [Unified Command Plan] mission to defend the Nation, as well as to support key geographic commanders like Admiral Paparo and United States Indo-Pacific Command (INDOPACOM).

We have a plan to take the six programs that are part of JCWA, that have currently been developed by the services, and to bring those underneath our program executive office, really focused on offensive, defensive and enterprise level operations, and it's working senator and I look forward to providing you and the committee additional updates on that.

Senator ROUNDS. Excellent. Senator Rosen.

Senator ROSEN. Thank you. I actually have a compound last question. So, I want a clarification on some terms that we use on about the PRC [People's Republic of China]. So, could you explain for the layman what "living off the land" tactics are and why it's important from a cyber defense perspective? The compound part of the question is, and finally, what do you really want us to know that we haven't asked you today. We know you've had just a short time to prepare for this, but maybe we'll give you that final word there too.

Lieutenant General HARTMAN. Hey, thanks, Senator Rosen. So, living off the land, you know, really describes when an adversary gains access to your network and then uses legitimate user credentials and legitimate user behavior in order to live in your network, in a way that makes it really hard to detect them using a standard antivirus or alert-based program.

Senator ROSEN. So secretly living in the basement, I suppose then, right?

[Laughter.]

Lieutenant General HARTMAN. It makes it really difficult because it's the behavior that you've got to detect. But look, we do know how to do that. We have gained a significant amount of knowledge. Artificial intelligence is going to help us, working with private industry is going to help us. And we're dedicated to continue to get after that problem.

Senator ROUNDS. Thank you. And then I think Senator King had one more question?

Lieutenant General HARTMAN. I didn't answer the second part of her question.

Senator ROUNDS. Oh, I apologize. Go ahead.

Lieutenant General HARTMAN. So, I think the thing that I would most like the Committee to take away is, Congress and the Department have given us authorities, right? They've given us Service-like authorities. They've given us control of the resources that apply to the ? one, so the Cyber Mission Force and the headquarters that employ them. We've been given acquisition authorities, we've been given joint force trainer authorities, and all those things are enabling us to evolve the command in a way that better enables us to compete with China or any other adversary. It is working. Okay.

There are things that slow down the process: continuing resolutions slow down the process, hiring freezes slow down the process, transitions between one combatant command support agency and the other, slow down the process. But we have a plan, we're executing it, and it's all about the ecosystem that we have to build that provides precise intelligence to really smart capability developers, that then field it to a force that has been trained and operationally aligned to receive that capability.

We're doing it with DARPA, we're doing it with the S&T community. We're doing it with the communities across our services that have significant investments in cyber capabilities. We're doing it based on operational requirements of geographic combatant commanders like INDOPACOM, and based on CYBERCOM requirements to defend the Nation.

So that's really the message I have here, those authorities, those resources, they're relatively new, but they are allowing us to really increase our ability to really get after all the things that we've talked about here.

Senator ROSEN. Thank you.

Senator ROUNDS. Senator King.

Senator KING. I realize this isn't exactly in your lane, but it's certainly close. You talked in your prior answer about the work with the private sector and alerting them to the threats and to what was going on, and that's very important. But the principal agency that actually has performed that function as an interface between the Federal Government and the private sector, is CISA [Cybersecurity and Infrastructure Security Agency].

My concern is that we've seen reports of cuts at CISA up to 90 percent. I believe 40 percent may be the latest number. and I think they've eliminated the office that interfaced with State election officials, that enabled them to share threat data and information and protections with State election officials to keep our election safe and secure.

I am just puzzled, at a time of heightened cyber threat, that we are essentially unilaterally disarming one of the most important tools that we have to protect ourselves in cyberspace. Do you have any views on the dismantling of CISA?

Lieutenant General HARTMAN. Senator King, thanks for the question. To be honest, I do not understand what the actual decisions are for any reduction or reorganization as it relates to CISA. I will tell you that we continue to talk to CISA leadership, and we continue to share information with CISA leadership as it relates to threats that are relevant to their mission for defenses in the United States.

Senator KING. Well, Mr. Chairman, I realize that again, this isn't his land, but this Subcommittee's dealing with the issue of cyber, and CISA is one of our most important tools to deal with that and they've been very effective. Having worked with some Members of the private sector that have worked with CISA, it took years to build a trusting relationship between this government agency and these companies, as well as the State election officials.

I remember when that initiative first started, and those State election officials were very reluctant to interface with this Federal Agency. But they became very—I wouldn't say dependent, but they became very engaged with CISA in the last several elections and to basically dismantle that capability, I think is very dangerous for national security at a time of heightened cyber-attack. We're under attack right now, and to be unilaterally disarming and disabling what amounts to a carrier fleet, I think is very damaging to the security of the country. Thank you.

Senator ROUNDS. I think Your concern is noted, Senator. With that, I want to thank General Hartman for coming in on short notice and participating in this Subcommittee hearing. This does conclude the open portion of today's cybersecurity subcommittee hearing.

I'd like to once again, thank our witness, Lieutenant General Hartman, for his testimony. For the information of Members, questions for the record will be due to the Committee within two business days of the conclusion of the hearing, and with that, Senator, any final remarks?

Senator ROSEN. No. Thank you for coming.

Senator ROUNDS. And with that, then this Subcommittee hearing is adjourned.

Lieutenant General HARTMAN. Thank you, Chairman, Ranking Member.

[Whereupon, at 4:27 p.m., the Committee adjourned.]

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR TOM COTTON

OFFENSIVE CYBER STRATEGY

1. Senator COTTON. Lieutenant General Hartman, what actions can U.S. Cyber Command (CYBERCOM) take as part of an offensive strategy to deter cyberattacks by China on our critical infrastructure?

Lieutenant General HARTMAN. Due to classification, please refer to the classified annex for this response.

2. Senator COTTON. Lieutenant General Hartman, what offensive actions can CYBERCOM take in response to new attacks on our critical infrastructure?

Lieutenant General HARTMAN. Due to classification, please refer to the classified annex for this response.

3. Senator COTTON. Lieutenant General Hartman, do you have the necessary authorities to conduct these operations?

Lieutenant General HARTMAN. USCYBERCOM has a variety of authorities that enable the Command to conduct Cyber Operations that may deter Chinese attacks on Critical Infrastructure and Key Resources (CIKR). These authorities include those contained in statutes and as authorized by the President. Existing authorities may be leveraged to conduct cyber operations for the specific purpose of deterring Chinese attacks on CIKR.

4. Senator COTTON. Lieutenant General Hartman, is the Department of Defense (DOD) able to effectively leverage the most innovative technologies for offensive cyber operations, and, if not, what needs to be done?

Lieutenant General HARTMAN. Due to classification, please refer to the classified annex for this response.

CRITICAL INFRASTRUCTURE

5. Senator COTTON. Lieutenant General Hartman, what are key trends in cyberattacks on our critical infrastructure in the past year?

Lieutenant General HARTMAN. In 2024, we observed an increase in criminal cyber activity in response to the conflicts in the Ukraine and Gaza. Ransomware attacks, some possibly linked to State actors, persist as a major threat to United States critical infrastructure. Incidents related to ransomware increased by approximately 9 percent from 2023.[1] According to FBI reporting, U.S. critical infrastructure companies (i.e. energy, manufacturing, healthcare and finance) experienced more cyber threats than any other sector in the past year.[2]

State actors continued to target common vulnerabilities in outdated hardware and software, with over 25 percent of vulnerabilities exploited within 24 hours of disclosure.[3] Despite the relative increase in ransomware threats against U.S. critical infrastructure, the average ransom payment decreased by almost 33 percent worldwide, suggesting efforts from the U.S. and global law-enforcement operations very

[1] FBI;2024—IC3Report; 23 APR 2025;(U) Federal Bureau of Investigation Internet Crime Report 2024; *https://www.ic3.gov/Annua1Report/Reports/2024_IC3Report.pdf;* Classification of extracted information is U; Overall classification is U.

[2] FBI; 2024—IC3Report; 23 APR 2025; (U) Federal Bureau of Investigation Internet Crime Report 2024; *https://www.ic3.gov/Annua1Report!Reports/2024_1C3Report.pdf;* Classification of extracted information is U; Overall classification is U.

[3] New Article;15 April 25; 159 CVE's Exploited in Q1 of 2025; *https://thehackemews.com/2025/04/159-cves-exploited-in-q1- 2025-283.html;* Classification of extracted information is U; Overall classification is U.

likely contributed to the decrease in profitability for ransomware operations, according to cybersecurity and open source reporting.[4][5]

Due to classification, please refer to the classified annex/or the remainder of this response.

6. Senator COTTON. Lieutenant General Hartman, do you think DOD needs more cyber-related information sharing with Cybersecurity and Infrastructure Security Agency (CISA) and other agencies?

Lieutenant General HARTMAN. DOD would benefit from more cyber-related information sharing across the government and with private industry, and vice-versa. Malicious cyber actors rarely target a single sector of the United States. The techniques tactics and procedures (TTPs) and indicators of compromise (IOCs) used against government and commercial entities are almost certainly relevant to all parties. Cyber-related information sharing between CISA and DOD exists, but authorities and information sharing agreements between military and government entities are bespoke and vary between agencies. Standardizing cyber-related information sharing across all Government and military entities would provide a more complete picture of adversary campaigns across the cyber spectrum. The result would be shared situational awareness for critical infrastructure, which would enable greater burden sharing and efficient response across the whole of government for cyber defense.

Due to classification, please refer to the classified annex/or the remainder of this response.

7. Senator COTTON. Lieutenant General Hartman, how would CYBERCOM's plans to partner with the Defense Intelligence Agency (DIA) help us defend and deter cyberattacks from China?

Lieutenant General HARTMAN. Due to classification, please refer to the classified annex for this response.

U.S. CYBER COMMAND CAPABILITIES

8. Senator COTTON. Lieutenant General Hartman, I'm concerned that CYBERCOM should be able to offer more significant combat power to the joint force. What are the biggest limitations to capability development?

Lieutenant General HARTMAN. Due to classification, please refer to the classified annex for this response.

9. Senator COTTON. Lieutenant General Hartman, what have been some of your greatest challenges when partnering with the private sector or academia to leverage the most innovative cyber capabilities and how can Congress help alleviate these challenges?

Lieutenant General HARTMAN. Navigating the complexities of the Defense Acquisition process is a challenge. For example, in our ongoing collaboration with the Defense Innovation Unit (DIU), we are working to unify the DODIN Hunt Kit and the CNMF Hunt Forward Kit under a common platform-the Joint Cyber Hunt Kit (JCHK). This effort involves leveraging multiple Research (IO US. C § 2371) and Prototype (IO US. C. § 2371b) Other Transaction (OT) awards to engage with industry partners in a nimble and collaborative manner. While the OT authority provides some flexibility, challenges remain in aligning government and industry timelines and ensuring sustained funding to support rapid innovation.

Another significant challenge is integrating cutting-edge technologies from non-traditional and non-Defense Industrial Base (DIB) companies into military operations. For instance, our strategic partnership with In-Q-Tel (IQT), a private, independent, and non-profit organization funded by the US. Intelligence Community, allows us to bridge the gap between venture capital companies, commercial startups, and government partners. Through this partnership, we can efficiently deliver critical technologies to the Cyber Mission Force (CMF). However, the rapid innovation cycles of private sector startups are often at odds with the deliberate pace of government acquisition processes. Additionally, small, non-traditional companies frequently struggle with navigating the complexities of the defense sector, including

[4] Article,Mandiant; 25-10005992; 10 FEB 2025; (U) Ransomware Payments Declined in 2024 Despite Massive Well-Known Hack; Classification of extracted information is U; Overall classification is U.

[5] Article,Recorded Future; 5 FEB 2025; *https://www.therecord.media/ransomware-payments-drop-2024-chainalysis-report;* (U) Ransomware Payments Drop for First Time in Years Following Law Enforcement Disruptions; Classification of extracted information is U; Overall classification is U.

strict regulatory and security requirements that can slow the adoption of innovative technologies.

USCYBERCOM also leverages Cooperative Research and Development Agreements (CRADAs) to conduct joint research and development with Federal Labs and non-Federal entities. CRADAs enable us to combine resources and collaborate with partners on cyber capability research.

The Software Acquisition Pathway empowers USCYBERCOM to rapidly acquire, develop, and deploy innovative software solutions, leveraging key partnerships with academia and the private sector. This agile approach accelerates the delivery of critical capabilities, enabling USCYBERCOM to stay ahead of evolving cyber threats and improve operational effectiveness. By fostering innovation and ensuring a more resilient and responsive cyber posture, these collaborations bring cutting-edge research and commercial expertise to bear on our Nation's toughest cyber challenges. This streamlined process allows them to experiment with emerging solutions, adapt to evolving threats, and maintain a technological edge. Your continued support for the Software Acquisition Pathway ensures USCYBERCOM, in partnerships with leading experts, has the tools needed to defend the Nation in the cyber battlespace.

ARTIFICIAL INTELLIGENCE

10. Senator COTTON. Lieutenant General Hartman, what are the most promising artificial intelligence (AI)-enabled cyber capabilities you are aware of and have you seen adversaries deploying these technologies against our Nation's critical infrastructure?

Lieutenant General HARTMAN. Due to classification, please refer to the classified annex/or this response.

11. Senator COTTON. Lieutenant General Hartman, how do you assess China's AI-enabled cyber capabilities?

Lieutenant General HARTMAN. USCYBERCOM assesses that AI is a pillar of China's military modernization strategy, which pursues the concept of "intelligent-ized warfare."

Due to classification, please refer to the classified annex for the remainder of this response.

12. Senator COTTON. Lieutenant General Hartman, have you shifted your strategy and investments following the release of DeepSeek?

Lieutenant General HARTMAN. Due to classification, please refer to the classified annex for this response.

13. Senator COTTON. Lieutenant General Hartman, as the DOD starts to increasingly use AI and partner with vendors that use AI, how is DOD ensuring a secure AI environment both at the Department and among partners in the Defense Industrial Base?

Lieutenant General HARTMAN. Due to classification, please refer to the classified annex for this response.

14. Senator COTTON. Lieutenant General Hartman, are there tools to automate or streamline compliance with cybersecurity requirement?

Lieutenant General HARTMAN. Current investment plans for AI adaption are not focused on resourcing non-operational usage, though tools to automate or streamline compliance are being evaluated. There are commercially available automated penetration testing tools.

POST-QUANTUM SECURITY

15. Senator COTTON. Lieutenant General Hartman, as we look forward to developments in the quantum computing field, what are we doing to advance quantum-resistant methods to protect the Department of Defense Information Network (DODIN)?

Lieutenant General HARTMAN. Due to classification, please refer to the classified annex for this response.

16. Senator COTTON. Lieutenant General Hartman, do you have the necessary expertise and resources to accomplish this?

Lieutenant General HARTMAN. USCYBERCOM will leverage the expertise resident in the NSA. NSA is responsible for cryptology for the Department of Defense, and as such they provide quantum-resistant methods for the Department.

TECHNICAL PERSONNEL

17. Senator COTTON. Lieutenant General Hartman, can greater automation or the use of AI-enabled tools help close the cybersecurity skills gap?

Lieutenant General HARTMAN. Greater automation and AI-enabled tools are essential to closing the cybersecurity skills gap; this is a capability we are deliberately building toward. At USCYBERCOM, we've outlined a strategic vision to integrate AI to enhance operator effectiveness, streamline cyber workflows, and expand the impact of our existing workforce.

While technologies such as AI-enabled copilots, agentic assistants, and low/no-code development platforms are not yet fielded, we plan to begin deploying them across mission areas in FY26 and beyond. These tools are intended to allow less experienced personnel to contribute more rapidly while taking on high value tasks to ease our reliance on hard to fill technical and institutional roles.

Due to classification, please refer to the classified annex for the remainder of this response.

MAVEN SMART SYSTEM

18. Senator COTTON. Lieutenant General Hartman, I understand that CJADC2 [Combined Joint All Domain Command and Control] and AI capabilities significantly enhance a commander's decision making and operational advantages. Have you utilized the Maven Smart System to achieve these benefits in your missions? If so, how?

Lieutenant General HARTMAN. Due to classification, please refer to the classified annex for this response.

○