RECORD VERSION

STATEMENT BY

HONORABLE KATHERINE SUTTON ASSISTANT SECRETARY OF WAR FOR CYBER POLICY

BEFORE THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

SECOND SESSION, 119TH CONGRESS

ON CYBERCOM POSTURE

APRIL 28, 2026

NOT FOR PUBLICATION UNTIL RELEASED BY THE COMMITTEE ON ARMED SERVICES

STATEMENT OF

MS. KATHERINE SUTTON

ASSISTANT SECRETARY OF WAR FOR CYBER POLICY

& PRINCIPAL CYBER ADVISOR TO THE SECRETARY OF WAR

TESTIMONY BEFORE THE

SENATE ARMED SERVICES COMMITTEE

APRIL 28, 2026

Introduction

Chairman Wicker, Ranking Member Reed, and distinguished members of the Committee, thank you for the invitation to testify to discuss the Department of War's (DoW) cyber posture and how we intend to operationalize the Department's priorities in cyberspace. I am pleased to testify alongside the new Commander of U.S. Cyber Command (USCYBERCOM), General Rudd; his immense experience especially in the Indo-Pacific theater will prove invaluable as we posture to implement the priorities outlined in the National Defense Strategy (NDS).

It is a privilege to also testify alongside the Assistant Secretary of War for Special Operations and Low-Intensity Conflict, Honorable Derrick Anderson, and the Commander, U.S. Special Operations Command, Admiral Frank Bradley. In many ways, we have sought to internalize the lessons learned from the special operations forces (SOF) community in how we organize for and conduct cyberspace operations. I believe jointly providing our posture statements is a testament to the Committee's recognition of how well these two functional areas work closely together, navigating the complexities of the global strategic environment.

In my role as the Assistant Secretary of War (ASW) for Cyber Policy and the Principal Cyber Advisor (PCA) to the Secretary of War, I oversee the Department's cyberspace operations policy and work with USCYBERCOM and the Services to ensure our cyber forces are organized, trained, and equipped to meet the ongoing and emerging threats to our nation. I come to this role with more than two decades of experience advancing our national security interests in the cyber domain, and from my time as a professional staff member, I have a deep appreciation for the importance of Congressional oversight. I look forward to a close and continuing partnership with the Committee to ensure we maintain the world's most elite cyber force, capable of achieving the President's vision of securing peace through strength.

Threat Environment

Cyberspace remains central to our way of life, proving essential for communication, global connectivity, economic prosperity, and innovation. As many of you are aware, the cyberspace domain is also defined by persistent, sophisticated, and aggressive cyberspace campaigns waged by malicious actors, including nation-states and criminal organizations. In cyberspace, this means we must operate every day to defend the Homeland and seek to continuously shape the battlespace on our terms.

Artificial Intelligence:

Artificial Intelligence (AI) is fundamentally reshaping the strategic environment by acting as a powerful force multiplier to increase the speed, scale, and sophistication of cyberspace operations. This is both an opportunity and a challenge. This is a decisive era where first movers who rapidly adopt AI will achieve comparative and competitive advantages over fast followers. Already, we are witnessing the advent of AI-enabled cyber effects and must seize the initiative to adopt, integrate, and leverage AI to its full potential across the range of cyber

operations – to outpace our adversaries who seek to employ AI for asymmetric gain across our free and open society.

In the last six months alone, industry threat analysis has demonstrated that threat actors in China, Russia, Iran, and North Korea are operationalizing AI for cyber. In February 2026, Google reported that threat actors are leveraging Gemini for all stages of the cyberspace operations lifecycle. It is imperative we adopt and integrate frontier AI at speed, putting the tools of AI into the hands of our cyber warriors to defend sovereign interests, deny adversary freedom of maneuver in cyberspace, and defeat malicious cyber effects that hamper Joint Force primacy, mobilization, or operational impunity.

As we integrate AI into critical infrastructure and national security systems, we must also prioritize securing AI models and the underlying "AI stack" from attack and misuse. AI models are vulnerable to compromise at every point in their supply chains, from the potential poisoning of initial training data to the manipulation of final deployment. As we adopt AI, we must ensure the security of models, agents, and data are assured. A multi-layered approach is necessary to build trustworthy and resilient AI that enhances human-machine teaming to meet the complexities of AI-enabled cyber warfare.

As we focus on building domain mastery in our cyber force, AI will allow us to economize and automate cyber activities in lower risk areas that cyber warriors currently do – and refocus cyber warriors on the exquisite, specialized skills they require to achieve mission agility for the cyber battlespace.

China:

China represents the most significant and multifaceted cyber challenge to the United States. Far beyond traditional espionage, China's cyber strategy focuses on the pre-positioning of disruptive capabilities within our most sensitive critical infrastructure. This marks a strategic shift from traditional cyber espionage, indicating preparation for potential future conflict by enabling China to disrupt military logistics, delay deployments, and exploit dependencies that DoW, our national security enterprise, and economic centers of gravity rely on.

Two distinct but equally concerning hacking groups that are state-sponsored by China, Volt Typhoon and Salt Typhoon, have executed tactics, techniques, and procedures (TTPs) to that end – with broad implications. Their persistence, even after discovery, poses significant challenges to vulnerability assessments, mitigation, eradication, and resiliency efforts due to the magnitude of cyber exploits across the shared critical infrastructure space between the public and private sector. The sophistication of these cyberspace operations, which include exploiting both known and zero-day vulnerabilities, exemplifies the undeterred nature of China's state-sponsored intent, capability, and capacity in this domain.

China continues to invest heavily in its technology sector and cyber workforce and will leverage AI, its command over its technology sector, and its talent base to accelerate and scale

capabilities to conduct cyberspace operations against U.S. critical infrastructure and government networks. China will not waver in its strategic commitment to developing capability to project power and achieve its geopolitical objectives through sustained and sophisticated cyberspace operations that traverse traditional notions of sovereign borders.

Russia:

Russia remains a formidable cyber adversary, adept at integrating its digital capabilities with military operations and geopolitical coercion. Russia employs a range of cyberspace operations, from espionage to cyber-enabled influence campaigns, to project power and sow discord within the United States and against our allies and partners. While Russia's cyber efforts are heavily focused on its military operations in Ukraine, it persistently maintains campaigns against North Atlantic Treaty Organization (NATO) members.

These operations serve not only to destabilize and gather intelligence but also to refine Russia's cyber warfare tactics. Although enhanced cyber defenses in Ukraine, supported by the United States and private sector partners, have successfully mitigated some of the most destructive attacks on Ukraine's critical infrastructure since the invasion began, the threat remains potent.

It is imperative that the United States and its allies and partners continue to strengthen collective defense and increase burden-sharing to counter Russia's malicious activities in cyberspace.

Other Malicious Actors:

In addition to China and Russia, a diverse array of additional state and non-state actors leverage cyberspace to threaten U.S. interests. Despite the setback to the Iranian regime caused by prior and ongoing U.S. and Israeli military operations, Iran continues to employ its cyber capabilities to target the United States and our regional allies and partners. In addition to amplifying anti-Western sentiment, Iran regularly uses proxies and front companies and has demonstrated a continued capability to maintain a breadth of simultaneous, campaign-like cyberspace operations to further its regional political and military objectives. Noting current operations, it remains to be seen the impact that Operation EPIC FURY will have on the regime's employment of cyber operations against the United States and key allies and partners in the region.

The Democratic People's Republic of Korea (DPRK) uses its cyber program as a critical economic tool, primarily to fund its weapons programs through large-scale cryptocurrency theft. According to Chainalysis information, in 2025, DPRK hackers stole more than $2 billion worth of cryptocurrency, bringing the cumulative amount of cryptocurrency assets it has stolen to over $6 billion. The DPRK can additionally raise funds by embedding IT workers within global firms. The DPRK has successfully leveraged AI to create convincing fake identities, thereby bypassing security and gaining insider access to Western firms.

Concurrently, the cybercrime ecosystem has rapidly industrialized, posing a significant threat to U.S. critical infrastructure. The proliferation of Ransomware-as-a-Service (RaaS) has lowered the barrier to entry for less-skilled criminals, allowing them to lease sophisticated malware and execute highly targeted strikes against high-value organizations. This evolution has shifted the landscape from opportunistic attacks to precise, damaging intrusions. Furthermore, the weaponization of AI is a growing concern across the spectrum of these threat actors, as it enables the automated development of malware, more effective victim selection, and the creation of hyper-realistic phishing campaigns that are increasingly difficult to detect.

Role of the ASW Cyber Policy & Principal Cyber Advisor

The Assistant Secretary of War (ASW) for Cyber Policy is assigned by statute, Title 10, U.S. Code (U.S.C.) Section 138(b)(9) (10 U.S.C. §138(b)(9)), to have as a principal duty "the overall supervision of policy of the Department of [War] for cyber," and as such is responsible for advancing the Department's strategic priorities in cyberspace. A key element of this responsibility is building a cohesive strategy for the Department in cyberspace; we work in close collaboration with other DoW components, our interagency partners, and a growing network of technology partners to take a collaborative approach to ensuring the Department's enduring advantages in cyberspace.

In addition to establishing the principal duty of the ASW for Cyber Policy, 10 U.S.C. §138(b)(9) also designates the ASW for Cyber Policy as the Principal Cyber Advisor (PCA) to the Secretary of War. As the PCA to the Secretary of War, the ASW for Cyber Policy, as provided in 10 U.S.C. §392a, is responsible for the overall integration of Cyber Operations Forces activities relating to cyberspace operations, including associated policy and operational considerations, resources, personnel, technology development and transition, and acquisition; and as provided in 10 U.S.C. §167b, exercises authority, direction, and control over the Commander of USCYBERCOM, with respect to the administration and support of USCYBERCOM, including readiness and organization of Cyber Operations Forces, cyber operations-peculiar equipment and resources, and civilian personnel, but does not exercise authority, direction, and control of operational matters that are subject to the operational chain of command of the combatant commands or with respect to personnel, resources, equipment, and other matters that are not cyber-operations peculiar and that are in the purview of the armed forces.

After completing a review of the organization during my first 90 days, I have re-focused the priorities and organization of my office to strengthen strategic oversight of cyberspace operations, improving accountability and policy execution across the Department.

To adapt to the evolving threat environment, we have refined our office by prioritizing engagements with industry to advance our competitive edge through innovative capabilities. This focus is especially critical at the intersection of AI and cyberspace operations, which presents both profound opportunities and significant risks. We are committed to working with

our partners at the Chief Digital and Artificial Intelligence Office (CDAO) and the Chief Information Office (CIO) to ensure that the Department stays ahead of adversary threats by integrating frontier AI capabilities urgently, yet with the appropriate safeguards. We are ready to implement the Department's AI Acceleration Strategy to incorporate frontier AI into every mission area to preserve military dominance.

Priorities & Strategic Vision to Implement the National Defense Strategy

The release of the 2026 National Defense Strategy (NDS) makes clear the Department's prioritization of achieving peace through strength by defending the U.S. Homeland, deterring China in the Indo-Pacific region through strength not confrontation, increasing burden sharing with allies and partners to address the myriad of threats facing the United States, and supercharging the defense industrial base. To meet the challenges of this era and to implement the strategic direction of the Department outlined in the NDS, my office is focused on three core priorities that will guide our efforts and investments. These priorities—Integrate Across All Domains, Gain Strategic Advantage in Cyberspace, and Organize to Dominate—are designed to ensure the Department's preparedness to deter conflict, protect our national interests, and win our nation's wars.

Integrate Across All Domains:

First, we must Integrate Across All Domains. Cyber is no longer a separate operational domain; it is the connective tissue of all-domain warfare. Cyberspace operations can achieve strategic effects without boots on the ground. It can disrupt adversary decision-making and create windows of opportunity for the Joint Force to exploit. Our objective is to seamlessly integrate and leverage cyber forces and capabilities across every warfighting domain to complement kinetic effects through non-kinetic options that buy down risk to mission and forces in conflict. The Department must continue to build our capabilities in cyberspace to provide the President and the Secretary increased optionality across the conflict continuum – options to respond to adversary threats in crisis so the United States can negotiate from a position of strength and ensure the Joint Force has every advantage in conflict to fight and win our nation's wars. There is no better example than what the U.S. military achieved in Venezuela by layering multiple effects to accomplish the mission with zero American lives lost.

We are building a cohesive cyber strategy that translates NDS priorities into activities and warfighting concepts that deliver lethal advantage. Success requires outmaneuvering and outpacing our adversaries in cyberspace while complementing the full suite of non-kinetic and kinetic capabilities in the U.S. arsenal. This cannot be done by the government alone. We are cultivating outcome-focused partnerships with increased burden sharing from our allies and partners, and with industry to generate measurable capability gains and ensure our collective defense.

Gain Strategic Advantage in Cyberspace:

Second, we must deny our adversaries freedom of movement in cyberspace. Our adversaries are persistently targeting our military, government networks, data and devices, defense industrial base (DIB), and critical infrastructure, and we will not let these actions go unchallenged. To do this, we will render our mission-essential networks as hostile terrain. This is the way we will secure our networks, through a whole-of-government effort and deep partnerships with the private sector. We will drive mission effectiveness by rapidly deploying cutting-edge technologies and delivering advanced cyber capabilities to our Combatant Commanders at the speed and scale required to deter and deny aggression, with a particular focus on the Indo-Pacific region.

However, a resilient defense, while one of the bare necessities, is only the foundation. A purely defensive posture is no longer sufficient in the current threat environment. To secure our interests, we must empower our world-class cyber operators across the full spectrum of cyber operations, signaling our resolve to contest active aggression in cyberspace that threatens U.S interests, our national security, and our way of life. We will enable our Combatant Commanders with a wider range of options that will be fully integrated with all other instruments of national power. Ultimately, our willingness to project power in and through cyberspace is essential to achieving peace through strength that will enable the Nation to preserve stability, U.S. military comparative advantage, and our national interests in an increasingly contested domain.

Organize to Dominate:

Third, we must Organize to Dominate. Our strategies are only as effective as the force that executes them. We are laser focused on forging a world-class cyber force capable of delivering superior lethality and warfighting outcomes. Through precise force design, generation, development, and employment, we are building a team of the most talented cyber operators in the world. This involves not only recruiting, training, and retaining elite talent, but also cultivating a culture of domain mastery, building specialized skills, and driving the mission agility required to deliver outcomes at the speed of cyber. True domain dominance requires us to translate this mission agility into action by shifting to a more dynamic force employment model, one where we can create and deploy purpose-built teams to meet any mission need.

Ultimately, these priorities work in concert to achieve a clear end state: to build and sustain robust cyber capabilities that enable the President and the Secretary of War to deter war, gain strategic advantage, defend our networks, and defeat adversary aggression, consistent with the NDS.

Private Sector Capability & Development:

To maintain our nation's competitive advantage in an era of accelerating strategic rivalry, our defense enterprise must be postured to move at the speed of innovation, not the speed of bureaucracy. This is especially true in the cyber domain, where the private sector is leading the way in developing the disruptive technologies that will define the future battlefield. The 2026

NDS clearly articulate that our current acquisition and development systems are too slow and must be reformed to keep pace with the rapid technological advancements emerging from the private sector.

We must continue to champion and implement historic acquisition reforms that cut red tape, empower program leaders, and lower the barriers for commercial and non-traditional companies to contribute to our national security. By prioritizing the adoption of commercial-off-the-shelf solutions and streamlining the cumbersome requirements process, we will ensure the Department is a preferred option for innovators and that we deliver cutting-edge capabilities to the warfighter on a timeline that is relevant to the threat, not one dictated by rigid processes that buy-down rather than accept risk.

Looking Ahead

Our People – Forging a More Lethal Force with CYBERCOM 2.0:

As I recently testified to the Cybersecurity Subcommittee, for several years, the Department has recognized that our approach to building cyber talent has not been keeping pace with the rapidly evolving and increasingly contested cyberspace domain. This misalignment has created significant challenges for the Department in recruiting the right people with the right aptitude and skillsets, retaining our most skilled and experienced operators in the face of lucrative private-sector opportunities, and providing the specialized, agile training needed to win against our nation's adversaries.

To address these systemic challenges, last fall the Secretary of War approved CYBERCOM 2.0, a fundamental reimagining of how the Department builds and manages our cyber forces. As he stated during his remarks at the Reagan National Defense Forum in December 2025, this represents the most comprehensive overhaul of USCYBERCOM since its inception 15 years ago. This initiative is not merely an incremental adjustment, but a deliberate and comprehensive overhaul designed to deliver greater operational outcomes for the Joint Force. CYBERCOM 2.0 efficiently synchronizes Commander, USCYBERCOM's authorities, as provided in 10 U.S.C. §167b, with the authorities and activities of the Military Departments. The core principles of mastery, specialization, and agility are indispensable for meeting our strategic objectives, irrespective of which organizational model ultimately emerges. At its core, CYBERCOM 2.0 is founded on these three fundamental principles that will drive the Department's cyber forces for years to come.

CYBERCOM 2.0 is the beginning of a necessary journey to build the cyber forces our nation demands. As a cornerstone of the Department's broader strategy, we will leverage this effort to re-imagine our cyber force design and employment models to deliver decisive operational outcomes for the Joint Force. At its heart, CYBERCOM 2.0 is a commitment to our cyber warriors, providing them with the careers, training, and support they deserve. By addressing critical force generation challenges, CYBERCOM 2.0 will significantly increase the

lethality and effectiveness of our cyber forces. Its purpose extends beyond cyberspace; it is a critical Joint Force capability that must be integrated across all warfighting domains, sending a clear message to our adversaries of our commitment to maintaining cyber superiority in support of our national interests.

Department of War Cyber Strategy & Action Plan:

To guide our efforts and ensure we are postured for the challenges of tomorrow, my office is leading the development of the 2026 Department of War Cyber Strategy and accompanying Action Plan. The singular objective of this strategy is to deliver the most capable, lethal, and agile cyber force in the world. This force will provide the President and the Secretary of War with a full range of options to deter conflict, achieve strategic advantage, defend our critical networks, and, if necessary, defeat adversary aggression decisively. This strategy will be fully aligned with the 2025 National Security Strategy, the 2026 National Defense Strategy, and President Donald J. Trump's forthcoming Cyber Strategy for America, ensuring our departmental efforts are nested within a clear, national vision, and move to action on NDS imperatives. Upon release, I welcome the opportunity to brief and partner with Congress on its implementation.

Conclusion

As I conclude, I would be remiss if I did not recognize the nexus of special operations and cyberspace operations. The synergy between these two communities is a powerful example of the future, creating an asymmetric advantage by presenting our adversaries with compounding dilemmas in both the physical and virtual worlds.

This partnership is critical because we are facing an unprecedented revolution in the speed and character of warfare. Cyberspace is our adversaries' preferred attack surface now and for the foreseeable future, and the 2026 NDS's imperatives highlight the exigency of this threat. Therefore, our response must be equally revolutionary. We must re-orient the entire cyber enterprise—our force design, force generation, and force employment—by integrating AI and shedding a purely defensive posture to seize the initiative. Our approach must be grounded in harnessing the engine of American industry, embedding lead-angle innovation directly into our operational architectures to secure our warfighting advantage.

Let there be no doubt: the Department of War's commitment to the defense of the nation is absolute. We have a solemn duty to ensure our Joint Force is equipped to dominate across all phases of conflict, to deter harm, and, when demanded, be prepared to answer any aggression with strength and resolve.

We will act as responsible stewards of the authorities you have entrusted to us, and I want to emphasize that the support of this Committee is not just appreciated, but it is fundamental to our mission success. Thank you, and I look forward to your questions.