Stenographic Transcript
Before the

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

TO RECEIVE TESTIMONY ON THE DEPARTMENT'S CYBER FORCE GENERATION PLAN AND THE ASSOCIATED IMPLEMENTATION PLAN

Wednesday, January 28, 2026

Washington, D.C.

ALDERSON COURT REPORTING
1029 VERMONT AVE, NW
10TH FLOOR
WASHINGTON, DC 20005
(202) 289-2260

TO RECEIVE TESTIMONY ON THE DEPARTMENT'S CYBER FORCE GENERATION PLAN AND THE ASSOCIATED IMPLEMENTATION PLAN

Wednesday, January 28, 2026

U.S. Senate
Subcommittee on Cybersecurity
Committee on Armed Services
Washington, D.C.

The subcommittee met, pursuant to notice, at 2:30 p.m., in Room SR-232A, Russell Senate Office Building, Hon. Mike Rounds, chairman of the subcommittee, presiding.

Committee Members Present: Senators Rounds, Ernst, Rosen, and Gillibrand.

OPENING STATEMENT OF HON. MIKE ROUNDS, U.S. SENATOR FROM SOUTH DAKOTA

Senator Rounds: I call this hearing to order. Welcome to today's Cybersecurity Subcommittee hearing on the Department's Cyber Force Generation Model, known more commonly as 2.0. The purpose of this hearing is to discuss how the DoD seeks to generate and sustain the advanced cyber workforce necessary to confront the full range of adversaries in the cyber domain scale.

I have about a five-page opening statement that I am going to submit for the record, because I want you all to have an opportunity to share with us how you are going to respond to this.

I think the most important part that we want to share is this particular approach is designed to provide us with cyber professionals to meet the workforce needs of literally a domain which is in huge demand right now, and has been the focus of anything having to do with military operations.

Today, as our witnesses, we have Katherine Sutton, Assistant Secretary of Defense for Cyber Policy, Office of the Secretary of Defense; Lieutenant General William J. Harman, USA, Acting Commander, United States Cyber Command and Performing the Duties of Director, National Security Agency, and Acting Chief of Central Security Service; and

Brigadier General R. Ryan Messer, U.S. Air Force, Deputy Director for Global Operations, J3 Joint Staff. Welcome to all of you. We look forward to hearing your thoughts, recommendations, and answer questions that we have of you.

And with that I will turn to our Ranking Member, Senator Rosen.

STATEMENT OF HON. JACKY ROSEN, U.S. SENATOR FROM NEVADA

Senator Rosen: Thank you, Chairman Rounds. I have a very short opening remark, so I am going to read those in and then we will get right to it.

This hearing is so important, and I appreciate the way that the Chairman and I worked together, hearing from all of you about the Department of Defense, your Cyber Force Generation Plan, the associated implementation plan, CYBERCOM 2.0. And for the witnesses here, thank you for your service and your commitment, because now more than ever the United States needs a cyber workforce equipped with the acumen and expertise to defend our networks, to executive offensive operations in a rapidly -- is not a fast enough word to even describe it -- a rapidly changing battle space that achieves our national security objectives.

I would point out, however, that the new National Defense Strategy, publicly released on Friday, only mentions cyber in three places. Cyber is everywhere. I am surprised at how little emphasis has been placed on cyber in comparison to other capabilities in the NDS. It does not engender much confidence that cyber is being treated with the necessary urgency or priority by this Administration that I think we would all agree that we

need.

The Department of Defense must take swift action to develop programs that enable our cyber warfighters to increase cyber domain mastery and operational readiness. It is critical. We have to promote standardized training across all of our services. We need a sustainable talent pipeline -- I know you are going to talk about that -- and we need effective initiatives for retention.

Because in an era of persistent cyber threats from foreign adversaries like China and Russia and Iran, they are probing and testing and challenging our systems, I would say by the nanosecond. Not even enough to say daily. Every single second. They are seeking any opportunity they can to degrade our command control, disrupt our operations, steal our most sensitive information, and they are using sophisticated cyber tactics to disrupt military operations, spreading dangerous propaganda to American citizens, and denying access to lifesaving goods.

Advancement in artificial intelligence by our adversaries, of course, they heighten the sense of urgency we must all feel right now, we must have to protect against AI-orchestrated campaigns aimed at targeting, well, targeting us, our critical infrastructure, our supply chains. And we cannot defend against these disturbing yet real threats without cyber professionals every step along

the way, armed with the requisite skills and abilities to bolster the cyber enterprise.

And so for too long the approach to manning, training, and equipping our cyber forces, we have just lagged behind, and we need to really step that up, in my opinion. The Department of Defense, we know we struggle, continue to struggle with recruitment, retaining cyber talent, particularly against such a competitive private sector. So this issue undermines our readiness across all domains, and it is a priority of this Subcommittee, and the Committee at large, to help the Department do everything that we can to fix it, because we cannot fight today's digital wars with the outdated infrastructure, with our inflexible personnel structures. We need a skilled, professional cybersecurity force. It is not a luxury; it is a foundational requirement for all of us.

So I am committed to work together in a bipartisan way, on this Committee, on the full Committee, with all of you, to be sure that we have the cyber force of the future that we need and will continue to need, going forward.

Thank you again for your work and for being here. Mr. Chairman, thank you.

Senator Rounds: Thank you, Vice Chair Rosen. Let me just begin with Secretary Sutton. We welcome you back. She has been on this side for quite a while, and we all

know you and appreciate what you do, and appreciate what you have already done in terms of providing for a lot of the language. But right now you operate under the International Defense Authorization Act that were implemented when you served on this side. So we appreciate having you back. We welcome you back, and we look forward to your opening comments.

STATEMENT OF THE HONORABLE KATHERINE SUTTON, ASSISTANT SECRETARY OF DEFENSE FOR CYBER POLICY

Ms. Sutton: Thank you. Chairman Rounds, Ranking Member Rosen, and distinguished members of the Committee, it is an honor to appear before you today. As you mentioned, it is really quite the privilege to be on this side of the table, representing the Department and all of the efforts that we are working forward to tackle those challenges that Senator Rosen highlighted in her opening remarks.

I am grateful for the opportunity today, in particular to discuss the Department of War's comprehensive efforts to organize, train, and equip our cyber forces to meet the complex changes the nation faces in the 21st century.

The subject of today's hearing, Cyber Command 2.0, represents what the Secretary of War, Secretary Hegseth, mentioned at the Reagan Defense Forum the most significant transformation of U.S. Cyber Command since its inception 15 years ago. This initiative is the cornerstone of our effort to ensure American dominance in a rapidly evolving cyberspace domain, meeting the President's clear mission to the Department of War, achieving peace through strength.

Cyber Command 2.0 is only one of the key initiatives we are to working to maximize our cyber forces. We are also working to validate, and if necessary, update our

force design and force employment to ensure we are able to achieve the maximum outcomes.

For many years, the Department has recognized that our approach to building and sustaining cyber talent was not keeping PACE. Our adversaries are investing heavily in cyber, while we have been constrained by traditional force generation models which, while effective for conventional forces, failed to fully address the unique requirements of cyberspace operations. This has created significant challenges in recruiting the right people, retaining our best operators, and providing the agile specialized training needed to win.

Our legacy force generation model is inconsistent, hindering our ability to adapt at speed and scale to counter threats like Volt Typhoon and Salt Typhoon, and quickly integrate emerging technologies like artificial intelligence.

To address these systematic challenges head on, the Secretary of War approved Cyber Command 2.0, a fundamental reimagining of how we build and manage our cyber forces. At its core, Cyber Command 2.0 is founded on three essential, fundamental pillars.

The first of those is domain mastery. We are shifting from a compliance-based paradigm to one that fosters deep, career-long expertise. Our goal is to cultivate a cadre of

cyber personnel who achieve true mastery through enduring operational experience rather than rotating through cyber assignments as generalists.

Second is specialization. The cyber domain is not one size fits all. Cyber Command 2.0 establishes dedicated pathways for our personnel to become deep experts in fields like industrial control systems or space asset protection, resulting in specialized units aligned to our most critical missions.

And third is agility. The cyber threat landscape evolves with unparalleled speed. We require a force that can adapt and employ new technology just as quickly. This model allows for dynamic allocation of talent, ensuring we maintain a proactive posture against the most pressing threats.

To bring these pillars to life we are implementing seven core attributes. The first is targeting recruiting and assessment. We are shifting from general recruiting to targeted talent acquisition, beginning with an in-service recruiting pilot using validated instruments like a Cyber Assessment Battery to identify individuals with inherent aptitude and suitability for cyber warfare.

Second are incentives for recruiting and retention. To remain competitive, we must implement robust incentive pay and retention bonuses that reward mastery, and we will

standardize this pay across the services.

Third is tailored and agile training. Through our Advanced Cyber Training and Education center we will focus mission-specific skills on demand, ensuring our forces remain ahead of technological advancements and adversarial tactics.

Fourth, tailored assignment management. We are engineering career pathways that enable sustained operator engagement, allowing operators to build a comprehensive portfolio of tailored experience rather than being forced to move on after a single tour. This approach generates domain mastery within the Cyber Mission Force while also providing greater operational effectiveness when warfighters return to their services and apply their developed talent to service mission sets.

Fifth is specialized mission sets. We are developing dedicated units of experts focused on highly specialized missions, such as protection of space assets or the defense of critical infrastructure, making them the world's leading authorities in their fields.

Sixth is integrated headquarters and combat support. Our tactical cyber teams will be presented with dedicated headquarters and combat support, ensuring they have the leadership and resources needed to execute their missions without the distractions they have today.

And last is optimized unit phasing. To prevent burnout and sustain readiness, we are instituting a unit phasing model that creates a sustainable operational tempo, keeping our personnel focused and effective for the long haul.

While each one of these attributes offers merit, the true power lies in their synergy, creating an exponential effect on our ability to generate and sustain cyber talent across the entire talent management lifecycle. These efforts are driven by the creation of three enabler organizations within Cyber Command, that General Hartman will talk about in his speech.

As directed by the Secretary of War, I will oversee the Cyber Command 2.0 implementation, consisting of 97 tasks across 26 lines of effort. This revised force generation model empowers the commander of U.S. Cyber Command to directly influence how our forces are manned, trained, and equipped, to deliver immediate warfighting outcomes while preserving decision space on future organizational constructs. The core attributes of mastery, specialization, and agility are indispensable, regardless of any future structural changes.

Cyber Command 2.0 represents the beginning of a necessary journey and the Department's commitment to providing our cyber warriors with the careers, talent, and

support they deserve. In addition to Cyber Command 2.0, the Department is undertaking several initiatives to enhance our warfighting capabilities in the cyber domain. They include validating and updating our cyber force design and developing a force employment model that ensures maximum lethality and operational outcomes.

Importantly, Cyber Command 2.0's purpose extends beyond the cyber domain. It is a critical Joint Force capability that must be integrated across all warfighting domains. This sends a clear message to our adversaries: the United States is all in on achieving and maintaining cyber superiority in support of our national interests.

Thank you for the opportunity to testify today. I look forward to continuing to work closely with this Subcommittee on this critical national security priority, and I welcome any questions that you have.

[The prepared statement of Ms. Sutton follows:]

Senator Rounds: Thank you, and I appreciate your comments, Secretary Sutton.

General Hartman, welcome, and as you get started I just want to personally say thank you for your dedicated service to our country and everything that you have done to forward our security through implementation of these types of policies in the cyber domain. And I appreciate that. Thank you, sir.

Go ahead with your statement, please.

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

General Hartman: Thank you. Chairman Rounds, Ranking Member Rosen, and distinguished members of the Committee, thank you for the opportunity to discuss the future of our nation's cyber force. Thank you specifically for the requirements in Section 1533 of the fiscal year 2023 NDAA that brings us here today.

The revised Cyber Force Generation Model approved by the Department is fundamental to a more lethal, agile, and enduring cyber force, capable of deterring, and if necessary, defeating our adversaries in cyberspace. CYBERCOM 2.0 directly addresses our national security challenges and fixes many of the issues facing our servicemembers. This is a significant upgrade in how we man, train, and equip the world's best cyber force.

Since the standup of U.S. Cyber Command we have had challenges manning the cyber force and ensuring we had viable cyber-centric career models across all services. We face many challenges, ranging from duplicative training, uncompetitive and inconsistent compensation, excessive administrative burdens, and a high operational tempo that contributes to an unsustainable stress on the force.

CYBERCOM 2.0 targets these problems through seven key deliverables that overhaul how the Department of War generates and sustains lethal cyber warfighters. These deliverables include overhauls in targeted recruiting, modernized incentives, specialized mission teams, and optimized operational tempos.

This plan gives us what we need. It forges cyber warrior by building upon the warfighting culture and lethal capabilities of the military departments, harnessing their institutional mastery of sustained warfare, their capacity for precise global operations, and their core competency and expeditionary and agile power projection in denied environments.

To lead this effort I have established three key enabling organizations. The Cyber Talent Management Organization is developing the cyber assessment battery test to better align incoming talent. To ensure we retain high-end warfighters, we are using our Title 10, Section 167b authorities to budget for standard skills pay and will next focus on retention incentives.

The Advanced Cyber Training and Education and Center is tailoring training to specialize mission needs while eliminating training redundancy in areas like artificial intelligence, expeditionary cyber, and advanced tradecraft.

Our Cyber Innovation Warfare Center will more rapidly

equip our cyber forces with cutting-edge capabilities and game-changing trade craft. We will build capabilities we need for the future, not focused on past requirements. This center will serve as the central point of collaboration for industry, academic, government partners, and the cyber operating force.

These enabling organizations are being designed to be AI by birth, built from the outset to be data centric, automated, and decision optimized. This means that data will be treated as a strategic asset, workflows are engineered for automation, artificial intelligence is embedded into planning, operations, and sustainment, not bolted on later.

Artificial intelligence is no longer a future concept. It is an operational capability we are integrating today. In line with our Cyber Command 2.0 vision, we are transforming how the command is organized, enabled, and resourced to operate at the speed and scale required in the cyber domain. We are fundamentally changing how we bring Thank you into the fight. Rather than relying on long, bespoke government development cycles, we are aggressively leveraging commercial proven AI technologies, the same systems driving productivity, analytics, and automation across the global economy, and rapidly adapting them for military use, while also building classified and mission-

specific capabilities internally, when required.

This industry-first approach allows us to move at the pace of relevance. It enables continuous iteration, rapid upgrades, and alignment with the global AI innovation ecosystem, which no single government entity can replicated on its own. In a domain where our adversaries are already exploiting automation and machine learning and large-scale analytics, speed is not a luxury. It is a necessity.

Importantly, we are no longer piloting AI for learning. We are operating AI for mission outcomes. Today AI is being used to accelerate cyber threat detection and response, prioritize and automate defensive actions across large networks, improve operational planning, targeting, and operations, and reducing analyst workloads so human expertise is focused on the highest value decisions. These are not experiments. These are capabilities already being delivered across the force.

Because getting this right is so critical, we have aligned our Chief AI Officer as a direct report to me, outside traditional stovepipes. This ensure AI data architecture and operational design are integrated from day one, rather than competing for priority after the fact.

CYBERCOM 2.0 strengthens our integration with other combatant commands. By building more proficient cyber forces, we provide more lethal and capable support to the

Joint Force. When our cyber operators are expertly matched to their roles, receive cutting-edge training, and are freed from administrative burdens to focus on the fight, their operational effectiveness increases exponentially. This enhanced capability directly translates to delivering decisive outcomes for CYBERCOM and other combatant commanders at the timing and tempo our senior leaders require.

In closing, I want to reiterate my appreciation for Congress' support and partnership over the past several years. Changes to our budget and acquisition authorities, as well as the fiscal year 2023 NDAA Section 1533 provided us the required tools and a clear mandate to address persistent readiness challenges and implement solutions across the Cyber Mission Force. We are using those authorities to implement CYBERCOM 2.0.

I assess implementing CYBERCOM 2.0 as the best path to get our cyber warriors and our cyber force where it needs to be to support the Joint Force, in crisis and conflict. The Secretary's direction is clear, and we have buy-in and participation with services. Alreqady we are leveraging the Army model for proficiency pay, and the Navy is implementing clear career progression for the maritime cyber warfare officers.

Your continued support, both in sustained investment

and providing flexible authorities to partner with the full spectrum of U.S. AI companies, from major defense primes to venture-backed startups, is what allow us to move fast, stay secure, and maintain our advantage. The success of this endeavor will depend on continued partnership with Congress and the Department to ensure adequate oversight and sustain funding to implement these necessary changes and maintain the world's premier cyber force. This is how we ensure that American innovation remains decisive in cyberspace.

Thank you. I look forward to your questions.

[The prepared statement of General Hartman follows:]

Senator Rounds: Thank you, General Hartman.

And General Messer, thank you. Welcome. I appreciate your service to our country. And with your statement, please proceed.

STATEMENT OF BRIGADIER GENERAL R. RYAN MESSER, USAF, DEPUTY DIRECTOR FOR GLOBAL OPERATIONS, J3 JOINT STAFF

General Messer: Chairman Rounds, Ranking Member Rosen, and distinguished members of the Subcommittee, thank you for the opportunity to join this hearing and speak to the importance of cyberspace as an integral part of joint all-domain military operations.

Joint Operations are reliant on operators who are masters of their craft. For example, an aviation strike operation requires aircrew who are exceptionally skilled in aerial refueling, air intercept control, air-to-air warfare, and strike warfare. It takes years of specialized training to build a team who can succeed in such mission areas. The same is true for our cyber operations.

At the same time, the demand for cyber forces across the Joint Force is steadily rising. As you will hear in combatant commander posture statements, our adversaries are using the cyber domain as part of their multi-faceted campaigns to degrade U.S. and allied interests. USINDOPACOM has emphasized defensive cyber operations as the "Joint Forces' first line in defense" in their theater, and USSOUTHCOM highlighted "cyber espionage" as a vector for both intelligence gathering and persuading audiences against U.S. interests in their theater.

Amid these threats, demand for cyber capabilities is

at an all-time high. Threats in cyberspace are currently growing faster than we can scale our actions. The size of the existing Cyber Mission Force requires us to prioritize some efforts and take risks in others, which could delay our response to meeting emerging threats.

For all military operations, actions in cyberspace are playing an increasingly important role. That includes operations where the cyber element may not be self-evident. Whether protecting our forces from harm, complementing kinetic action, imposing costs on adversaries, or defending friendly infrastructure, cyberspace operations are critical to the successful employment of the Joint Force. To succeed, we must be proactive, not reactive. Cyber activities must be integrated into every phase of operations, starting with concept development.

Military operations in every domain require specialists. Just as specialized aircrew support every air operation, specialized cyber operators are essential to ensure U.S. dominance in cyber and all-domain operations.

CYBERCOM 2.0 will help us combat the adversary's ability to mass forces with domain mastery and advanced tools, extracting the greatest value from the force that we have. Training, experience, tools, and resourcing will give our operators what they need to prevail in this dynamic domain.

On behalf of the men and women of the Joint Force, we appreciate your support for the Cyber Mission Force and for this vital initiative. And with that we will open it up for questions.

[The prepared statement of General Messer follows:]

Senator Rounds: Thank you, General Messer.

Look, to begin with, we are in an open session right now so we have an opportunity to not only ask questions but to help educate, as well. Five domains -- air, land, sea, space, and cyberspace. It appears that there will never be another kinetic activity that does on in terms of our Department of Defense or Department of War without having some cyber activity to the left of it, basically to make the field of battle a little bit safer for our young men and women.

But in order to do that it has to be integrated and a part of the larger force. And in order to make that happen, you need professionals that clearly understand their role. That is lot about what this discussion today is about. It is about the cyber force itself and how they actually provide the needed services to different COCOM commanders, combatant commanders, that we lay out throughout the world. In order to do that, we have got to make sure that the cyber operations can be integrated as quickly and as efficiently as possible.

Ms. Sutton, part of the CYBERCOM 2.0 initiative recommends maturing the Assistant Secretary of Defense for Cyber Policy position to meet the demands of executing Section 167b authority for cyberspace operations peculiar activities. And I just want you to describe what that

maturation might look like in practice. Specifically, how would an enhanced Assistant Secretary for Cyber Policy, how would that office support the force generation objectives outlined in CYBERCOM 2.0, and what additional responsibilities or authorities would be necessary to effectively execute this expanded role? In other words, what specific resourcing would be required to enable that maturity of the ASD Cyber Policy office?

I know you are new in the role and so forth, but you have got a great deal of experience in the cyber domain and what we have done within the National Defense Authorization Act in the past. Your thoughts, please.

Ms. Sutton: Senator Rounds, than you for that really important question. So as you mentioned, one of my top priorities going forward, and what I think one of the key responsibilities of my office, is to make sure that cyber is integrated into multi-domain operations. And so having this role be fundamental and be embedded within the Under Secretary of Policies organizations allows that to happen on a daily basis, to bring the cyber domain to all of the policy discussions happening more broadly.

I think historically we have seen cyber treated very much in a stovepipe, where the cyber people go off and talk about the cyber domain and do their things in a silo and in a vacuum. And I see one of the primary roles of my office,

both as the Assistant Secretary for Cyber Policy as well as the principal cyber advisor in my role to be an advisor to the Secretary of War, is to be that coordinating function across the Department, to really bring cyber to all of the other domains of warfighting, to coordinate across the services, and to look for opportunities where resourcing is needed and where we need to really focus the Department's efforts to achieve these outcomes that are going to be critical to all future conflicts going forward.

Senator Rounds: Thank you. And just in order to make sure that all of our members get an opportunity to speak, and we are going to do several rounds of questions, I will defer right now to Senator Rosen.

Senator Rosen: I am going to defer to Senator Gillibrand, because we are here the whole time and everyone has a lot of hearings going on. So Senator Gillibrand, you are recognized.

Senator Gillibrand: Thank you, Mr. Chairman. Thank you, Madam Vice Chairman.

General Hartman, since the fiscal year 2017 NDAA, CYBERCOM has had the authority over the training of assigned joint forces, conducting specialized courses of instruction, monitoring and promotion of Cyber Operation Forces, coordinating with the military departments regarding assignment, retention, training, education, and

special and incentive pays for Cyber Operation Forces. The command has been the Joint Force trainer for almost as long. Much of CYBERCOM 2.0 appears to be tinkering with this space rather than fundamental reimagining. Can you speak to why the command did not take these steps before and why you believe this is a dramatic transformation?

General Hartman: Senator, thanks for your questions. As you point out, in 2017 we were given certain authorities. But what we did not have control of at the time was the funding, Senator. So as you are aware, in 2023, we were given enhanced budget control. There were a series of issues that actually caused us to not receive control of that funding until 2024. And so when we had some authorities we really had no enforcement mechanisms, and we have started to execute those enforcement mechanisms, and we have seen benefit from that.

Senator, CYBERCOM 2.0 does not intend to totally reinvent how we train the force, but what it does intend to do is make sure that the services are held to the standard of 1,000-level training. The CYBERCOM J7 will continue to execute 2,000-level training. So basic training by the services, qualification through CYBERCOM, which we have made a lot of progress on in the last 2 years. And then what CYBERCOM 2.0 is really going to bring is advanced and specialized training, moving at the pace of industry, that

is really required, that will allow us to both compete and really plan to outpace China. That is the construct that we are laying out, Senator.

Senator Gillibrand: Thank you. Secretary Sutton, while the services largely say cyber is important, it is not a top priority for any of them. Agreeing to a notional plan is easy, but the services are notoriously protective of their control over their recruiting, retention, and talent management. How will your office hold services accountable and ensure they do not steamroll CYBERCOM on career and talent management?

And I will just say that this Committee, we have had hearing after hearing, year after year, and we have drilled down to how many personnel you are getting from each service, and which services are slower than the other, and what level of staff you could acquire. And frankly, it is never good enough. So I just really want to know how you intend to succeed?

Ms. Sutton: Senator, I appreciate your question and understand the frustration. I think you are really highlighting what is fundamental about Cyber Command 2.0, which is involvement at the Secretary's level to really coordinate and make sure that the services are all doing things consistently and that we rise everybody to the top bar.

We see best practices in pockets across the services, but have historically lacked a coherent effort to bring all those together and rise all levels up. It is going to require hard discussions internal to the building. It is going to require prioritization. And we have a clear direction from the Secretary of War when he approved this plan about the importance of increasing the lethality of our cyber warriors.

I look forward to having all those internal battles within the Pentagon, because I think it is fundamental to what we owe our cyber warriors that come to work every day and do this mission, is to be able to train them and retain them in ways that allow us to maintain the world's most competitive cyber force.

Senator Gillibrand: General Hartman, it was just reported that China improved the import of H200 chips to ByteDance, Alibaba, and Tencent. These companies all work closely with Chinese military, and just a few months ago reports indicated a White House memo raised concerns that Alibaba provides support for PRC military operations against targets in the U.S.

If these sales go through, what impacted will this acquisition of H200s have on their ability to target U.S. military and U.S. critical infrastructure?

General Hartman: Senator, I have not studied that

question, so I will agree to get back to you with an answer.

Senator Gillibrand: Thank you. And just my last point. I would like to hear from each of you. I still do not understand why you do not want a Cyber Academy. I just do not know why you do not want a service academy that will just train the personnel you need, from top to bottom, consistently and regularly. We tried to create small pipelines for you through Cyber Academy for non-military personnel, but I still do not know why you do not want your own. I get why you are going to use existing services and try to do better training, but future war is going to be cyber, and I do not know why we are taking so long to do this.

And I think also in your testimony you said that your goal for -- what is the group? -- the ACTEC, the Advanced Cyber Training and Education Center, will not be fully operational capable to Q3 fiscal year 2031. I mean, that is a really long time for any bricks and mortar.

But can you each talk about why you do not have this vision, and why is it so difficult?

Ms. Sutton: So I really appreciate that question because I think how we get the right training to our people and what courses we have available and what mechanisms we have is really important.

I really want to highlight the importance in Cyber Command 2.0 of the ACTEC, the Advanced Cyber Training and Education Center. And the intent of it is actually not to be a brick-and-mortar institution, because what we see is having an internal developed training system is probably always going to be slow to need. As we look at the timelines it takes to get basic training updated, we are losing out to the best of breed that is happening in industry and academia. So that Advanced Cyber Training and Education Center model is really intended to figure out what our requirements are, where we have skills and key knowledge gaps that we need training on, and then to be able to go out to industry and academia, find the best of breed, if it is available out there, bring that in, and then we can have standards that we are trained to.

So that is really the model that we are looking to move out on quickly. The timelines that we are talking about are to get it fully up and scaled across the entire force, across an entire curriculum. I will let General Hartman talk about some of the early pilots that we are aiming to get some quicks wins in.

Senator Gillibrand: Again, the Chairman can take control of this, but honestly, we have been saying that for a decade, and it just does not work. We cannot compete. We do not pay enough. Our salaries are too low. So the

benefit that the service academies have is it is free college for 4 years, or 2 years, or whatever it is going to be. So kids will choose to do that route because we can compete on that.

Let's say you set your standard, every 6 months of the perfect person. They are not going to join you, because they are making $400,000 or $600,000 where they are. You are not going to get them.

So you guys can answer the question if you want, but you can also take the time back if you would like, Mr. Chairman.

Senator Rounds: I will allow the question, if you have got it, and if not we can bring it back in and you can respond with a written response. But I would be curious to hear what your thoughts are on it.

Ms. Sutton: Just one thing and then I will let General Hartman also provide his answer. I am a firm believer in exactly what you mentioned. I am a Scholarship for Service recipient. My master's degree was funded through government funds with a service obligation, and over 20 years later I am still in government. I see it is a very powerful recruiting tool and something that we are continuing to look to opportunities to continue to leverage.

General Hartman: Senator, I am not opposed to a joint

cyber service training academy. I think there is great merit in that. What I do not think is the best answer right now is to divorce our cyber capability in the Department from the services. And that is based on everything that we are doing from an operational standpoint. And if I have got to build a cyber plan against an adversary's air defense network, the Air Force, as a service, brings tremendous capability to me that I do not believe we need to separate.

Senator Gillibrand: Got it.

General Hartman: And then the second piece is, the Advanced Cyber Training Academy, what we are trying to do is really marry the training to the operational elements of the command. So we learn things in an Ops Room, both offensive and defensively, that we immediately turn into a training requirement, that we train across the force. So each disparate element is not learning every time they get on keyboard in order to execute operations. We just think that is fundamentally important, but there is a huge institutional training environment, and I support your idea.

Senator Rounds: Thank you, Senator Gillibrand, for the excellent questions. I appreciate that.

Ms. Sutton and General Hartman, you are likely aware of the calls -- and this follows the same line -- for the

establishment of a separate military service dedicated to the cyber domain or a cyber force. Like me, you are no doubt close with and respect many of those who are supportive of a cyber force. What would you say to those national security and cyber experts who are advocating for a separate cyber force? Step right into it.

Senator Rosen: You knew he was going to ask that, didn't you?

Ms. Sutton: I appreciate that question. I think this is a really important debate for us all to be having about the future of the cyber warfighting domain. I do think one of the most common misconceptions about Cyber Command is that it is a debate between Cyber Command 2.0 and a cyber force, and they are actually separate debates that I believe both need to be had, and we need to look closely at the pros and cons of both.

Cyber Command 2.0 is inherently about building a talent model. It is looking across the entire talent pipeline from when we recruit someone, how we make sure we have the right talent, how we train them, how we retain them, how we build careers for them, how we really build our cyber warriors. We know how to do this. As Cyber Command has become operational we have built a set of very capable cyber operators. Now we need to do that at scale and have a system that supports that, rather than doing it

in an ad hoc method.

And so Cyber Command 2.0 is really that talent management model, and we have been very careful as we have built that model that it is agnostic to the organizational model and that it would support both the current model, where five services present, as well as other organizational models, such as the establishment of a cyber force.

So I think they are both really important debates to have, but they are separate debates that we need to make sure that we are quickly moving ahead with Cyber Command 2.0. We have a lot of work done, and it is required regardless of what model we have. We have to build the talent. And so that is our immediate focus, is working on all of these fundamental activities that we are going to need, going forward, that would enable any future decisions to be made about an organizational change.

Senator Rounds: General Hartman?

General Hartman: Chairman, I just would like to add three things to what the Honorable Sutton said. I agree with her that this CYBERCOM 2.0 is certainly important regardless of any future decision.

I do believe when we did the analysis for CYBERCOM 2.0 the timeline was fundamentally important, so we did view this through a 2027 lens. We viewed it through a

resourcing lens. And through that lens, CYBERCOM 2.0 provided us the best opportunity in order to build the force that we needed on a 2027 timeline. And I think that is important.

The second piece is, I fundamentally believe the ability to integrate across the Joint Force is best suited to the model that we are developing here in CYBERCOM 2.0, and that is fundamentally important. I did not answer the question that you asked earlier, but our ability to integrate not just left of conflict but during a conflict, in all phases of the operation, just like any other traditional military capability, is absolutely essential to us delivering the capability that the nation needs. And I think CYBERCOM 2.0 is really the best course to do that.

Senator Rounds: And I am going to be asking a question in a little bit about some of that, the cyber activity that might occur during an operation, as well.

But I do want to follow up a little bit. With CYBERCOM 2.0, where does a civilian workforce fit into a CYBERCOM 2.0 concept?

Ms. Sutton: So the scope of Cyber Command 2.0 is primarily focused on the Cyber Mission Force and it is enabling organizations, the headquarters, Cyber Command headquarters, the Joint Force, Cyber headquarters, which is a blended workforce of both military and civilian and

contractor work roles. So as a result, within Cyber Command 2.0, the majority of initiatives do apply to both military and civilian populations, and we have sort of dedicated lines of effort that also target some things that are unique to both sides. So in short, we are addressing both issues for those elements that support the Cyber Mission Force.

Senator Rounds: Plenty of room for Guard units to continue to participate?

Ms. Sutton: Absolutely. The Guard and the Reserve are going to be critical on how we bring in some of that unique talent that has special expertise, and there are specific lines of effort in the implementation plan where we look at how to bring that in, as well as they will be a fundamental part of our cross-functional team that we are building to roll out the implementation.

Senator Rounds: Senator Rosen.

Senator Rosen: Thank you. Well, you actually set me up for my next question, you did not even know. But I want to thank you for the testimony so far, because cyber is not an add-on or service adjacent anymore. It has to be part of the fabric of everything we do, woven in.

And talking about data, I always say this data tells a story if you know how to listen to it. And so I hope that we can maybe have a hearing to talk about how we think

about data and its role in everything that we do going forward. That is a separate issue.

But I actually want to talk about the servicemembers, to what Senator Rounds was talking about. So I have two questions for you, General Hartman. One is on the regular force and the second one is on the Guard and Reserve.

The first one, can you talk a little bit how you build a fully qualified cyber operator? What does the training pipeline look like at service and joint level, and what kind of on-the-job experience is required before they can be deemed full qualified, and how often do they, I guess, have their benchmarks taken, I guess if you think of it like that.

General Hartman: Thanks, Senator. Each of the services produce a cyber operator, and that is a blanket term. We have a number of different specialties across the force. And then we, CYBERCOM, supervise what we call work role training. So if you are an interactive on-net operator you go to a specific training course. If you are an exploitation analyst or another specialty you would do the same thing. And we work through a process that allows them to meet a series of benchmarks and then become fully qualified. Once they become fully qualified they execute a series of operations and move from basic to journeyman to master level of qualification.

Historically, we have not produced a lot of operators at the master level, because the training and the certification process has taken too long. And part of CYBERCOM 2.0 is how do we reduce that training timeline and allow them to focus more on operations vice less on qualifications.

So I think we have, over the years, reduced that benchmark, but you get trained, you get qualified, you execute operations, you become a noncommissioned officer, and then you supervise the next group of people that we are bringing up.

It is a process that works, but it does not work fast enough, and that is really the focus of 2.0 and the ACTEC program.

Senator Rosen: Thank you. I want to ask a similar question about the skills for our National Guard and Reserve members. They are not currently tracked, it is my understanding, at the same fidelity as the active force, so they are going to be a critical part, to your point, of bringing in the public sector, I guess, if you will, say it that way.

So what specific steps, can you talk to us about how you are going to ensure that a Guardsman or Reservist with those high-end cyber skills, they might be doing it in the regular world, their civilian career, how can they be

activated for special mission? How are you working with that? Because I do think that is a big part of our pipeline and training. So whatever, you both can answer, please.

General Hartman: Thanks, Senator. We do have organizations in the National Guard that are exemplars that we are trying to really use to leverage it across the entire Reserve component. We have got the Delaware and the Maryland Air National Guard that is part of our Cyber National Mission Force. So one of our most elite organizations really for the last decade. We bring those servicemembers on active duty and they participate as full members of the team. To be honest with you, they bring deep expertise, because when they are not mobilized, as you highlighted, they go back to civilian jobs.

We have an organization down in Texas supporting our Air Force cyber organization that, again, provides a significant amount of expertise. And we have the same model on the defensive side.

What we have to do is scale that across the force. We have got to get them all in JCC2-R, our readiness tool, and we have got to be able to track them just like we are tracking our active duty servicemembers.

Senator Rosen: Because you may, across the country, each state may have one or two that are working in this

area in their civilian life. And so how do we pull them in?

General Hartman: Senator, that is our plan. We are in the relatively early stages, but as we build this out, that is our intent.

Senator Rosen: Thank you. Senator Rounds.

Senator Rounds: Thank you. General Messer, you have gotten off too easy so far. I am going to throw you the hard one now, and this is sitting in an unclassified setting. I want you to talk a little bit about successes, and I want to specifically talk Venezuela.

It has been in the news, there has been a lot of discussion about the fact that this was a good example of what happens when you combine all of the Joint Forces, including cyber operations. Once again, I understand that this is an unclassified, but there are a lot of folks out there that might now have a curiosity about this, and they may very well want to be a part of a team in the future that you are going to have to try to recruit.

Can you share with us -- and I would open up to anyone else, as well here -- can you share with us the types of operations and how this happened -- it is not just at the national level or the international level or the big picture, strategically, but tactically, how critical cyber is when you are doing -- and this was a law enforcement

operation -- but a required support of the armed forces of the United States. Can you share a little bit about what that meant for the cyber teams involved? And a no answer is not acceptable.

General Messer: Senator, thanks for the question. What I probably will not do is go into specifics of the Venezuela operation. But what I will tell you is as has been mentioned by Honorable Sutton and General Hartman, the role that they play as leaders in pushing cyber to the forefront I think is critical. And that is one of the things we have seen from Chairman Caine, is his emphasis on not just traditional kinetic effects but the role non-kinetic effects play in all of our global operations, especially cyber.

So leading up to the events in Venezuela over the last 6 months we have been developing something new on the Joint Staff called a non-kinetic effect cell. This is designed to integrate, coordinate, and synchronize all of our non-kinetics into the planning and then, of course, the execution of any operation globally.

I think it is important to point out that one of the reasons that it has been successful is the emphasis that the Chairman has placed on the role of non-kinetics and, in particular, cyber, and then the coordination that has continued to grow and mature with CYBERCOM as we work

through various operations around the globe.

Senator Rounds: So in this particular case, not only was there a huge amount of work to be done beforehand, but then it had to be executed at the time, as we say, not just on the left side but during the operation itself.

For young men and women that are out there and they want to be involved in a growing and very exciting field, can you talk a little bit about what that means in terms of why we want these folks to actually be a part of not just the large Cyber Mission Force but actually within their own branches, and the need to maintain that continuity and understanding of the big picture by individuals who are back in with their regular units, and how that gets integrated in terms of providing direct assistance on a unit-by-unit basis. How integrated is this? As a member of the Joint Forces, I just kind of wanted to hear you talk about how critical that is.

General Messer: Yes, sir. Cyber operations are critical to everything we do, whether it is just day-to-day operations of the functioning of the Department of War or it is actual execution and operations.

One of the things that I will point out is growing up in the Air Force there was always a non-kinetic effect cell at an Air Operations Center, but it usually existed back in a back room, it was a very dark place, and usually we did

not ask for many inputs from that team until we wanted to sprinkle what we called the lightning bolts onto some form of operation. The reality is that we have now pulled cyber operators to the forefront.

So if I were talking to a group of young people who were considering a career, and joining General Hartman's team over at CYBERCOM, I would say, "You are not just going to be integral to every option we are going to do, but you will be at the forefront of everything we do, both now and in the future."

Senator Rounds: So let's just say that there is a young man or woman out there, and they enjoy the keyboard work, and they are fascinated by cyber. They have seen what hackers do. Is there a place for the good guy hackers to be, and how would they be able to let you know that they want to go to work for you? What is the best way to get that word out?

General Messer: Sir, I think there would absolutely be a role for them to play, and I think that the targeted recruiting and assessments that will be a focus of CYBERCOM 2.0 will open up more of those opportunities to find those unique individuals. And I wanted to see if General Hartman wanted to say more about that.

General Hartman: There is a place for them to go, Chairman, absolutely. Our intent is part of CYBERCOM 2.0

is if you are a young person, a hacker, you want to come serve your country when you show up at your recruiting station, we want you to be administered a cyber aptitude test. If you score well on that test we would like you to be offered a contract to become a cyber operator in whatever your service of choice is. And we would like you to then go through the pipeline and come to CYBERCOM. That is the first way.

The second way is we are going to execute an in-service recruiting pilot. And so if you are out in another specialty, the same way that you might attract a Delta Force operator in the Army, we are going to also give you an aptitude test, and if you meet a certain score on that aptitude test we are going to work with your service to have you move to the Cyber Operational Force.

And so we believe those two areas are ways that we can really attract world-class talent.

I do want to go back, if you allow me, to just address a little bit the question you asked the J39. I would tell you not just Absolute Resolve but Midnight Hammer and a number of other operations. We have really graduated to the point where we are treating a cyber capability just like we would a kinetic capability. We are not sprinkling cyber on. We are integrating cyber operations into the Joint Force Commander's plan, and we are executing it to

achieve specific effects that are ultimately tied to what the commander is trying to achieve, and we are doing it in a repeatable, sustainable manner, across a number of different COCOMs.

So while we cannot go into detail here, Chairman, I would love to get an opportunity to brief you in some level of detail. I do believe it is fundamentally one of the reasons we created CYBERCOM, and I do believe we have achieved a certain level of integration that is really important for our nation.

Senator Rounds: Thank you for that. And we will make arrangements to have a classified meeting, and we would invite you to come back and share that with the members of this Subcommittee. Thank you for that. Senator Rosen.

Senator Rosen: Thank you. I can tell you, the young woman who started her career in computer programming in 1980-something could not dream of what is happening now and what have been so excited about all the things that you are doing or having even been recruited. Of course, these things did not exist in the same way they do now. So I can tell you all those folks are out there, because if the wayback clock, if you went back, that would have been something that would have excited me, and it still excited me to this day to think about it. Cyber is kinetic capability. It is in the fabric of everything we do. We

use it the same as every bit of intelligence and every bit of capability, and it is really important.

But I just want to ask, I think, the last question I am going to ask. How do we leverage security automation tools to defend our DoD networks? We are talking a lot about the pipeline. We know we have more to go to recruit and train and figure out how we are blending all of this together so it is seamless, in the same ways that we do a lot of our intelligence capabilities, right.

But I want to just move for a second to security automation tools. General Hartman, you have to defend those DoD networks. It is fundamental, right? And so I had a provision in the Cyber Defense Command to s subordinate unified command included in the fiscal year 2025 NDAA. It is a structural change that reflects the sophistication of the current threat landscape.

So as our adversaries increasingly utilize AI, as we talked around the circle about AI, to execute cyberattacks at machine speed, the Department's ability to maintain real-time visibility over the DoD information network is being tested like never before. So detecting a vulnerability, it is only half the battle, right? You know you have a vulnerability, and now you have got to close the door. So it requires a speed that manual process may not be able to achieve.

By deploying security automation tools, can we move from a reactive posture to a proactive defense that keeps China, Russia, other adversaries off our networks, and how you are factoring in this use of automation and AI into CYBERCOM 2.0 for our developing cyber operators who defend the network?

General Hartman: Senator, thanks for the question. First of all, thanks for the legislation as it relates to DCDC and a subunified command. I assure you, General Stanton has taken that legislation and is running with it, and certainly implementing that.

Look, the use of automation, artificial intelligence in order to secure the Department of War information network is absolutely a part of CYBERCOM 2.0 and our plan for the defense of the DoD. It is not going to entirely take the human out of the loop, but what it is going to do is identify the most important data that our analysts need to look at in order to best protect our network.

We have executed a number of pilots, one I think we previously briefed called an Optic Junction, that the Army executed down at Fort Gordon. We are looking at scaling that technology. It was specifically focused about how to find Chinese living off the land techniques, that we have seen repeatedly used.

But the bigger piece, though, is really closing the

loop between what we learn in our offensive capability and what our defensive teams are prepared to defend against, and literally, in real time, turning around that knowledge so that as we learn more, we use that information to drive our own defense of our networks, and artificial intelligence and automation is absolutely, 100 percent part of our plan.

Senator Rosen: Thank you.

Ms. Sutton: If you would not mind if I added in just one additional comment.

Senator Rosen: Of course.

Ms. Sutton: one of the things that I am really excited about with Cyber Command 2.0 is the Cyber Innovation Warfare Center, or the CIWC, which is really looking at how do we adopt all the innovation that is moving very rapidly in this domain, particularly AI and automation, and how do we operationalize that most effectively in the Department.

So it is not just about acquiring a tool or a technology. There are a lot of non-material aspects that we will need to be successful. How do we need to train our workforce to most effectively use that tool? AI is going to change fundamentally what many of our work roles do in this domain, so how do we develop new training modules? What doctrine, what new tactics, techniques, and procedures

do we need to develop to be able to fully leverage these new capabilities?

So the model of the CIWC is to have an Innovation Warfare Center that can look at technologies that are going to have game-changing effects in our domain, bring in the operational input that General Hartman mentioned, and in a very short term, look at how we need to address everything we need to adopt that technology, both material and non-material, and then get that into our platforms as quickly as possible.

It will be our tie to industry. It ties our operational force directly to industry, to allow this to happen at the speed at which we are seeing the capabilities come out.

Senator Rosen: No, I could not agree more. Thank you for that answer. I do think artificial intelligence will potentiate what we can do, help us do it faster, maybe a little bit smarter. But it will help us pull it all together. Thank you for that.

Senator Rounds: General Hartman, just a follow-up with regard to the response that you gave to Senator Rosen. One of the items that you talked about was kind of term of art when you say the Chinese are living off the land. Since this is an open meeting and it is going to be broadcast, can you share a little bit about what that means

for folks that are out there, about how that works, what that means?

General Hartman: It just means that the Chinese have executed a deliberate campaign in order to compromise U.S. networks, and they use negative commands and native features inside those networks to move around, to look like legitimate traffic that makes it difficult for us to find those.

Senator Rounds: Is it fair to say, just confirm, they would be within our telecommunications systems today?

General Hartman: So have seen them in telecommunications systems. We have seen them in critical infrastructure. That is the bad news. The good news is we see them, and we report them, and we execute operations to get them out of those networks. And increasingly, as we build expertise under the CYBERCOM 2.0 program, it will allow us to do that more effectively.

Senator Rounds: Thank you. I am just curious, as well, I am thinking now about universities across this country, and I am going to use an example in South Dakota, Dakota State University, where they produce, perhaps, 400 cyber professionals per year. They have jobs basically before they are out of school. They are in the Madison/Sioux Falls area in South Dakota. But a lot of them want to be a part of providing cyber protections.

You have, and you need to be able to do not only cyber protection, defensive capabilities for the Department of Defense's programs, but you also then do offensive stuff, as well, and you need tools for both. Can you talk a little bit about what you have for capabilities in terms of getting young people involved in the development of those specific tools? And these are tools that are not just traditional cyber tools but ones that have basically been agent-ized, for lack of a better term, using AI as a part of that process.

Can you talk about the need for that and the availability for young people out there that want to be involved in this, who may not necessarily want to be directly involved full-time, but either through Guard units or through a civilian contract, and your interest in actually having them make contact with you along that line?

General Hartman: Absolutely. So in the command, in our service components, each of those organizations have development organizations, and those development organizations work specifically with operational teams in order to produce capabilities. To date, that effort has not been as unified as we would like. It is one of the key work roles that we talk about. When Honorable Sutton talked about the CIWC, the CIWC is really going to be the organization that brings our service development units

together and ensures that they have the absolute best training and they have access to the best development environments, they have modeling and simulation capabilities to really look at what are future capabilities. In each of those organizations we have both military and civilian members, and certainly there is an opportunity to work there. Across a number of our Reserve component units, we partner with them from a development standpoint.

But I think that the latter part, Chairman, is where we really have to move forward with CYBERCOM 2.0, and it is how do we partner with cutting-edge, innovative, private companies that we can work with in order to produce capabilities that we need in order to execute operations. And as I said in my opening statement, this probably is not the extremely large defense firms. It is these smaller organizations, often times made up of members that used to be in the Cyber Mission Force, or as part of the intelligence community. And we are working with a number of those organizations right now in order to do that.

Senator Rounds: Thank you. Senator Rosen?

Senator Rosen: So you need the developers of the software for the end user, so this is where you are writing application software. This is where the collaboration between a software developer and your end user is, because

we do not want to give you what we think you need. We want to give you what you actually need. So these are where the conversations about creating what you need, and the person goes to write that software for you, or however that gets done, or gives you the tools to let that happen dynamically with giving you the framework and they can put in certain particulars. So I am very excited about you doing this.

That leads me to the question we always ask. What do you need from us? So you might need new authorities. You might need incentives -- retention incentive payments, rotational programs, other legislation, things with the private sector, expedited clearance perhaps, if you are going to be using folks from the private sector.

So we are going to be working. We are working on the NDAA, this next years, right, as we speak. So as you think about this, what are some things, off the top of your head, that will help us with readiness, workforce retention, private sector? What do you need from us as we go back and think about our next hearings, to get us ready for our good mark?

Ms. Sutton: I will start out by saying how grateful we are for all of the things you have given us. I think there has been significant focus over the last 5 to 7 years on additional authorities, additional funding, additional pay. I think the Department, at this point, has a

significant obligation to execute all of those, and I think we are on a good path to do that.

At the moment, we have not identified any specific new authorities that are necessary. A lot of it is implementing the authorities and really maturing and fully leveraging the authorities that we already have. But do appreciate the offer, and intending that we will continue to work with you iteratively as we work through the implementation of Cyber Command 2.0, and identify things that we do need. You will be the first ones to know, and we will gladly get you that information.

Senator Rosen: Anything else?

General Hartman: I agree with Honorable Sutton. We appreciate all the additional authorities that we have been offered. We appreciate your advocacy for funding. It will be important as we implement 2.0, as we really build out the capabilities that we need from an artificial intelligence standpoint.

I do believe there will be a discussion about how do we best fund the activation of our Reserve component forces, to ensure that we can do that in a sustainable, repeatable manner, that we are able to bring the talent to the active force in order to execute specific missions. There have been some good use case examples, but it is a system that is not optimized, and I do think we will work

with the Department and Congress on how we might like to do that better in the future.

Senator Rosen: So like my Civilian Cyber Reserve idea, perhaps.

General Hartman: I think it is a great idea, Senator.

Senator Rosen: General, you wanted to add something?

General Messer: Ma'am, I was just going to say thank you very much for the support that you have provided. I reflect what Honorable Sutton said of, you know, you have been exceptionally supportive. I think it is now time to fulfill CYBERCOM 2.0's objectives, and then from there continued support from Congress is much appreciated. Because as you both pointed out, this is a part of warfare in the 21st century, and will continue to be. So your support and advocacy, as well, is tremendous. So thank you.

Senator Rosen: Well, I know I am thankful for your work and everyone that works with you, and I am especially grateful to be Ranking Member with Senator Rounds. Because on this Committee, we just see cyber on this Committee, right? And so it is really a pleasure to be able to think about these things in a meaningful way, going forward. Thank you, Mr. Chairman.

Senator Rounds: Thank you, Senator Rosen. And it is bipartisan, and it needs to stay that way. And we need to

look at how we fully mature this particular protection within this particular domain. I appreciate your help and the cooperation that the entire members on both sides have done in moving this forward, as clearly evidenced by the amount that we are getting done in each of the NDAAs over the last couple of years. So we appreciate that. Thank you.

With that, this will conclude the open portion of today's Cybersecurity Subcommittee hearing. Questions for the record will be due to the Committee within two business days of the conclusion of this hearing. And General Hartman, I will take you up, at some point in the future we will set aside time for a classified hearing to learn a little bit more about the processes and the procedures that you did use so successfully. Thank you.

General Hartman: Thank you, Senator.

Senator Rounds: Thank you all for your sacrifice and service for our country. And with that, this Committee meeting is adjourned.

[Whereupon, at 3:41 p.m., the hearing was adjourned.]