

[H.A.S.C. No. 118-68]

HEARING
ON
NATIONAL DEFENSE AUTHORIZATION ACT
FOR FISCAL YEAR 2025
AND
OVERSIGHT OF PREVIOUSLY AUTHORIZED
PROGRAMS
BEFORE THE
COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES
ONE HUNDRED EIGHTEENTH CONGRESS
SECOND SESSION
—
SUBCOMMITTEE ON CYBER, INFORMATION
TECHNOLOGIES, AND INNOVATION
ON
**CYBER IN AN ERA
OF PERSISTENT ENGAGEMENT:
THE FISCAL YEAR 2025 BUDGET REQUEST
FOR U.S. CYBER COMMAND AND CYBER
OPERATIONS**
—

HEARING HELD
APRIL 10, 2024



U.S. GOVERNMENT PUBLISHING OFFICE

56-081

WASHINGTON : 2025

SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES,
AND INNOVATION

MIKE GALLAGHER, Wisconsin, *Chairman*

MATT GAETZ, Florida
LISA C. McCLAIN, Michigan
PAT FALLON, Texas
DALE W. STRONG, Alabama
MORGAN LUTTRELL, Texas
JENNIFER A. KIGGANS, Virginia
NICK LALOTA, New York
RICHARD McCORMICK, Georgia

RO KHANNA, California
SETH MOULTON, Massachusetts
WILLIAM R. KEATING, Massachusetts
ANDY KIM, New Jersey
ELISSA SLOTKIN, Michigan
JARED F. GOLDEN, Maine
PATRICK RYAN, New York
CHRISTOPHER R. DELUZIO, Pennsylvania

JOSHUA STIEFEL, *Professional Staff Member*
MICHAEL HERMANN, *Professional Staff Member*
BROOKE ALRED, *Research Assistant*

CONTENTS

	Page
STATEMENTS PRESENTED BY MEMBERS OF CONGRESS	
Gallagher, Hon. Mike, a Representative from Wisconsin, Chairman, Subcommittee on Cyber, Information Technologies, and Innovation	1
WITNESSES	
Haugh, Gen Timothy D., USAF, Commander, U.S. Cyber Command; Director, National Security Agency/Chief, Central Security Service	4
Manning, Ashley, Performing the Duties of the Assistant Secretary of Defense for Cyber Policy	3
APPENDIX	
PREPARED STATEMENTS:	
Haugh, Gen Timothy D.	45
Khanna, Mr. Ro	27
Manning, Ashley	29
DOCUMENTS SUBMITTED FOR THE RECORD:	
Gallagher, Hon. Mike	63
WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING:	
[There were no Questions submitted during the hearing.]	
QUESTIONS SUBMITTED BY MEMBERS POST HEARING:	
Mrs. McClain	87
Mr. LaLota	89
Mr. Wittman	92

**CYBER IN AN ERA OF PERSISTENT ENGAGEMENT: THE
FISCAL YEAR 2025 BUDGET REQUEST FOR U.S. CYBER
COMMAND AND CYBER OPERATIONS**

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON CYBER, INFORMATION
TECHNOLOGIES, AND INNOVATION,
Washington, DC, Wednesday, April 10, 2024.

The subcommittee met, pursuant to call, at 3:33 p.m., in room 2212, Rayburn House Office Building, Hon. Mike Gallagher (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. MIKE GALLAGHER, A REPRESENTATIVE FROM WISCONSIN, CHAIRMAN, SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION

Mr. GALLAGHER. The subcommittee will come to order.

This will likely be my final hearing as chairman of the subcommittee. And before we get underway, I want to thank—well, he is not here. I was going to—I had this whole nice thing prepared to thank Ro Khanna for his partnership. We will have to save all the sappy stuff for when he actually gets here. But he is amazing, and we have had a great partnership.

And being on this committee for 8 years has been a highlight of my time in office, and I want to thank all the members. And Matt and I have sat next to each other for 8 years now and had a lot of late-night debates during NDAA [National Defense Authorization Act] markup, and I have—and often collaborations when it comes to AUMF [Authorization for Use of Military Force] issues. And I have sincerely enjoyed that.

So today we are going to—we are going to hear from the Department on its budget request and plan for cyberspace operations for the coming fiscal year. From 2013 to 2023, Congress tried to address force design and readiness through 24 different pieces of legislation, civilian and military workforce issues via 45 separate provisions of law, and cyber security at the Defense Industrial Base in 42 provisions of law. That is a lot of activity.

Through this latest NDAA, we incorporated new requirements, reports, and mandates into each of those same categories, and yet here we are. There are still significant issues with our force design, our civilian and military workforce issues remain as challenging as they have been in the past 10 years, and several cyber incidents targeting the Defense Industrial Base have demonstrated that we are as vulnerable now as we were a decade ago.

And just as I said when we were here a year ago for this same cyber posture hearing, insanity is doing the same thing over and over again and expecting different outcomes. I believe that almost everyone here today is familiar with a report published just 2 weeks ago by the Foundation for the Defense of Democracies on the issue of a cyber force, a proposed new branch of the armed forces dedicated to the cyber domain.

This new force would be responsible for organizing, training, and equipping for the cyber domain, no different from the Navy for combat at sea or the Air Force as the service responsible for air warfare.

The report is very compelling. And, as I said, in an event we did a couple of weeks ago, I came in as a skeptic, but I think they have raised some very important issues that need to be addressed, and it is a debate that is worth having because I think the status quo right now is unacceptable.

But the arguments were not—the cogent arguments in the report are not the only thing that stood out. Included in the report were personal accounts provided anonymously by more than 75 active and recently separated service members representing every military branch and rank from E-7 to O-7 as well as senior civilians. Not a single individual that was approached declined to respond, nor did any one of them argue in favor of the current approach in which the operational force is sourced from four separate military services.

I, therefore, ask unanimous general consent to enter this report into the record. So ordered.

[The information referred to can be found in the Appendix on page 63.]

Mr. GALLAGHER. I will admit, again, I had concerns at the start of this debate, but over the last 18 months I have been presented with an astounding array of data and arguments in favor of a cyber force, as well as a number of convincing arguments opposing such a force. In my mind, the most logical way to address this question is a fully independent evaluation of the notional cyber force to be led by an entity other than the Department of Defense—other than the Department of Defense is critical.

If anyone is opposed to a study of this question, I believe there is only one way to interpret that opposition, which is that if you are unwilling to ask the question, what you are really saying is that you are scared of the answer you might receive and the actions we will have to take to address the problem. When it comes to national security, that way of thinking—acceptance of risk because of fear—I think is unacceptable.

And while I may not be chair of this subcommittee during this year's NDAA markup, I hope my colleagues will make the right decision and work collectively to ensure the Department of Defense is directed to conduct such a study when the time comes.

With that as context, I am very eager to hear from both of our witnesses—thank you for being here—each appearing for their inaugural cyber posture hearing. There is a whole set of elaborate initiation events that we have to do afterwards. It is highly top secret. But we are joined by Ms. Ashley Manning, a career senior executive performing the duties of Assistant Secretary of Defense for

Cyber Policy, and General Tim Haugh, the Commander of the United States Cyber Command. Thank you both for appearing today.

At this point, I would turn it over to the ranking member. He is not yet here. Here is on his way from an oversight hearing, but I ask that his opening remarks be entered into the record. I ask unanimous consent for that to happen, and then something magically happens and it goes into the record.

[The prepared statement of Mr. Khanna to can be found in the Appendix on page 27.]

Mr. GALLAGHER. And, with that, we go to Ms. Manning first, correct, for 5 minutes.

STATEMENT OF ASHLEY MANNING, PERFORMING THE DUTIES OF THE ASSISTANT SECRETARY OF DEFENSE FOR CYBER POLICY

Ms. MANNING. Chairman Gallagher, Ranking Member Khanna, and distinguished members of the committee, thank you for inviting me to testify on the Department of Defense's cyber posture and the advancements we continue to make operationalizing the Department's priorities in cyberspace. It is an honor to appear alongside General Haugh.

In my role Performing the Duties of Assistant Secretary of Defense for Cyber Policy, I am committed to providing overall supervision of the Department's policy for cyber, advancing the Department's strategic approach to cyberspace, and ensuring our readiness to counter emerging cyber threats.

Mr. Chairman, I look forward to working with this committee through my newly established office to further these objectives.

I come to this role as a career civilian with almost 20 years of service in the Department of Defense. I have had the privilege of working across a wide range of regional and functional issues, serving most recently as the Acting Deputy Assistant Secretary of Defense for the Middle East and the Principal Director for Plans and for Posture. And in my previous positions, I have witnessed the cross-cutting role cyber plays in the defense of our Nation and our allies and partners.

The President has nominated Dr. Michael Sulmeyer as the ASD [Assistant Secretary of Defense] for Cyber Policy. Should he be confirmed, I look forward to serving as the Principal Deputy Assistant Secretary of Defense for Cyber Policy.

Our National Defense Strategy makes clear that the People's Republic of China remains an enduring cyber threat and the Department's pacing challenge in cyberspace, as the PRC [People's Republic of China] continues to target U.S. networks in prolonged campaigns of espionage and to pre-position its cyber forces for future operations.

Russia remains a persistent threat to the United States and our allies and partners, as it continues to leverage cyberspace to target critical infrastructure networks and enable its malign influence operations. The ongoing, unprovoked, further invasion of Ukraine serves as a stark reminder of Russia's willingness to employ cyber capabilities to disrupt defensive military operations and sow discord.

Following Hamas's attack against Israel on October 7 of last year, Iran has exploited cyberspace to create additional disruptions and challenges in Israel. While many of these malicious cyberspace activities have been relatively limited in their impact, the ability of both state and non-state actors to act against Israel in the immediate aftermath of the attack by Hamas is a reminder of what to expect in future conflicts.

Additionally, the United States continues to face the still-growing threat posed by for-profit cyber criminals that target a wide array of vulnerable sectors, conducting ransomware attacks that impact the daily lives of Americans across the country.

In response to these evolving challenges, the Department issued its fourth DOD [Department of Defense] Cyber Strategy last May. Looking ahead, we are committed to implementing our strategy and monitoring progress through the forthcoming cyber posture review in fiscal year 2026.

We understand the Department cannot advance its defense priorities without a ready, capable, and informed joint force. To achieve this end, we will invest in our people, in our capabilities, and in our information needs to support and enable the full range of cyber activities.

In partnership with USCYBERCOM [U.S. Cyber Command], we are refining options for the secretary on how to improve the way in which forces are presented to the command to raise the readiness level of these forces and to streamline support mechanisms to other combatant commands. These options will enable USCYBERCOM to fully exercise authorities in partnership with my office, including through enhanced budget control.

As part of the fiscal year 2026 budget cycle, DOD released its first-ever Department-wide Cyber Operations Programming Guidance. This guidance will shape future cyberspace operations investments and will serve as a rubric for my office's certification of the budget's adequacy for fiscal year 2026.

With the authorities granted to us by Congress, the Department will continue to build on the pathway laid out in the fiscal year—or, I am sorry, in the 2023 DOD Cyber Strategy to provide a stronger cyber posture and protect the shared digital environment for those who intend to subvert our values and our interests by pursuing integrated deterrence, which includes our cyber capabilities.

The Department will be ready to fight and win the Nation's wars with an ability to rapidly respond across the spectrum of conflict. Thank you for your continued support in this fight, and I look forward to answering your questions.

[The prepared statement of Ms. Manning can be found in the Appendix on page 29.]

Mr. GALLAGHER. Thank you.

General, you are recognized for 5 minutes.

STATEMENT OF GENERAL TIMOTHY D. HAUGH, USAF, COMMANDER, U.S. CYBER COMMAND, DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE

General HAUGH. Chairman Gallagher, Ranking Member Khanna, and distinguished members of the committee, thank you for the op-

portunity to testify before you today. I am honored to testify beside Ms. Manning. Joining me today is Chief Master Sergeant Kenneth Bruce, the U.S. Cyber Command and National Security Agency Senior Enlisted Leader. We are honored to represent the men and women of U.S. Cyber Command.

In an era defined by rapid technological advancement and increasing interconnectedness, cyberspace has emerged as a vital domain for protecting our national security. The People's Republic of China is our greatest strategic competitor and poses unique challenges due to its advanced cyber capabilities, state-sponsored cyber operations around the globe, and a strategic focus on leveraging cyberspace for military, economic, and political purposes.

Russia's cyber espionage campaigns prioritize sensitive U.S. Government and military infrastructure and information and spread disinformation campaigns to influence public opinion and undermine our democratic processes. Iran, North Korea, terrorist organizations, and transnational criminal groups also challenge U.S. interests in cyberspace. And we are engaged in ongoing efforts to exploit vulnerabilities—and are engaged in ongoing efforts to exploit vulnerabilities in U.S. networks, conduct influence operations, and erode our national security interests.

With cyber operations becoming more sophisticated and frequent, it is vital to evolve our capabilities against new and novel threats. I am confident Cyber Command is well postured to meet the ever-evolving challenges we face today, creating advantage for the Department and the Nation.

Our mission is to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners.

We defend forward by countering cyber threats before they can reach U.S. networks and critical infrastructure. These proactive defensive measures ranging from network hardening and threat hunting to information sharing bolster the resilience of our systems and foil potential cyber attacks before they can materialize.

We are aligned with the National Defense Strategy and the DOD Cyber Strategy to protect Department of Defense information systems, support Joint Force commanders with cyberspace operations, and defend the Nation from significant cyber attacks.

I am excited with what 2024 means for the maturation of U.S. Cyber Command. This is a year of opportunity for us, and I would like to thank Congress for the service like enhanced budget control authorities granted by the 2022 NDAA and enacted with the fiscal year 2024 appropriation. This authority creates tighter alignment between requirements and acquisition, which will result in faster capability and fielding for our cyber mission force.

Additionally, this committee has been instrumental in focusing attention on readiness across the cyber mission force. The studies you have authorized are driving us to do work needed to ensure we have the force structure and force generation strategy necessary to field a force of the highest quality today.

I hope we have an opportunity to unpack several of these initiatives today. Since Cyber Command's elevation in 2018 to a unified combatant command, Cyber Command has worked to make most of its authorities, resources, and support. Of these authorities, None

is as vital to national security and the command as Section 702 of the Foreign Intelligence Surveillance Act, which is essential for identifying malicious cyber actors in protection of the Nation and the Department of Defense.

I am confident we are successful in our mission each and every day thanks to our people, our innovation, and our partnerships—my top three priorities that ensure we deliver outcomes against national priorities in foreign intelligence and cyber security.

First, our strength lies in our people. Skilled cyber warriors who are dedicated to protecting the Nation from threats posed by our rivals and adversaries in cyberspace. We win because of our people.

Second, Cyber Command remains committed to a relentless approach in innovation to strengthen our military, now and into the future. Our investment in technological innovation is key to maintaining our overmatch against our adversaries.

Lastly, Cyber Command maintains our competitive advantage through sustained and deliberate partnerships. In addition to the unique partnership of the National Security Agency, Cyber Command further embraces a team approach, working with my fellow combatant commanders and interagency partners while also collaborating with academic and industry experts, and cooperating with our allies and partners by establishing collective security.

I am extremely proud of the efforts Cyber Command has achieved and the direction we are headed. I look forward to your questions.

[The prepared statement of General Haugh can be found in the Appendix on page 45.]

Mr. GALLAGHER. Thank you, General. You expressed, I believe, that the Section 15—I am recognizing myself for questions, in case that was not apparent. The Section 1533 study was looking at all options, to include the establishment of the separate service and, hence, a separate analysis isn't necessary.

But we required the Department to do the study in the 2020 NDAA, specifically to study the independent service idea as part of the cyber posture review. It seems to me that DOD ignored that requirement and then pointed us to a section in the posture review that included an assessment. But if you look at that section, no such assessment existed.

With this as context, I guess we will, one, address that. But why should we believe that the Department will follow on with an objective analysis as part of the 1533 study, given that it was ignored previous to this.

General HAUGH. Chairman Gallagher, I have no experience with the 2020 study. I can tell you what we are doing today. So we have taken that direction, and we have really—that is an area for us that is really about the readiness of our force, and how do we generate our force. So we have looked at that, in combination with other studies that you have asked us to do this year.

So there are other studies to look at our headquarters, to look at our acquisition force, to look at how we examine our architecture. And each of those we think make up a really good opportunity for us to evaluate what is the future of this force. So specific to your question on 1533, and the study that is underway, the book-ends that are required by the law are the way it was done last year

and an evaluation of a cyber service. We are going to look at both of those bookends, and then look at options in between that would allow us to generate the force that we need.

The other things that I think are—that I know we are doing today is the partnership we have with ASD Cyber, who is the other portion of the study. So being done with ASD Cyber in OSD [Office of the Secretary of Defense] and Cyber Command. We owe that to the secretary in June, and we are required to brief him in June the results of that study, and we are moving at pace to ensure that we look at all of the options that you directed.

Mr. GALLAGHER. Now, I am on record as favoring something like a zero-based budgeting for congressional studies because they accumulate over time, and periodically we need to sort of clear them out. But when they are a matter of U.S. law, they should be complied with.

Ms. Manning, do you know how many congressional requirements DOD is currently delinquent on?

Ms. MANNING. Thank you for your question, Mr. Chairman. This is actually one of the first questions I asked when I got into the seat. And we are tracking 12 reports where our office is the office of primary responsibility to be able to conduct and conclude these reports.

I received a status update on all of these reports. There are a couple that have been delayed because they were independent studies that were dependent on getting funding, and because of the continuing resolutions it has gotten delayed a little bit. But my commitment to you is to make progress on all of these reports and ensure that we are delivering them as quickly as possible.

I would note that there are a myriad of other reports related to cyber that have been directed across the Department, and we are providing support as a coordinating entity on many of those reports. And, in the interim, if there are specific issues where you want to understand a bit more about what the Department is doing and how we are addressing issues, myself and my team are always willing to come up and brief you on those.

Mr. GALLAGHER. I appreciate that. We are tracking 40, but that may be a broader aperture than just your office, but we very much would like to clear the backlog and work with both of you on clearing the backlog, because, again, wherever those reports appear it means that we—you know, we voted on it. We had a debate on it, and it means there is questions we just need answers to. And so I just would welcome your commitment to clearing that backlog.

Ms. Manning, your office will also be assuming the responsibility for certifying the cyberspace operations budget within DOD. Last year we were informed that the fiscal year 2024 cyber ops budget was 7.4 billion, but then this year the fiscal year 2025 ops budget, if I am correct, is 6.4 billion.

What we are trying to understand is, does this represent a net decrease or a confusion about categorizing investments? Can you share your view of what appears to be a net reduction of nearly 1 billion or more than 15 percent of the overall budget?

Ms. MANNING. Thank you for your question on our budget, because it is really important that we get this right. So my understanding is that overall our cyber activities' budget has increased

by almost a billion dollars due to added investment in cyber security. The teams in both policy and in the Office of the Chief Information Officer reviewed the various efforts that are included in the different budgets and decided that certain portions of the cyber ops budget are actually better categorized as part of the cyber security budget. So there is no reduction. It is more of a recategorization of some of the activities that we are funding between the different budget categories.

Mr. GALLAGHER. Thank you. My time has expired.

Mr. Khanna is recognized for 5 minutes.

Mr. KHANNA. Thank you, Mr. Chair. Apologies for being a few minutes late. We had an oversight hearing where I had to vote.

General Haugh, great to see you again. I appreciated our conversation the other day.

And, Ms. Manning, thank you for your testimony.

General Haugh, one of the things that we had discussed is the importance of getting young talent into our military service, particularly young talent in technology. The military can also be a place where they develop initial skills and training, something that may be more accessible, frankly, for people than just starting in Silicon Valley, which often does not have as, unfortunately, broad-based hiring.

Can you talk about efforts at creating recruiting programs at community colleges or historically black colleges, Hispanic-serving institutes, and other public universities across the country, that would allow us to recruit folks and perhaps even recruit folks who may not have a 4-year degree?

General HAUGH. Certainly, Ranking Member Khanna. This is our important issue is, how do we grow talent and for—for U.S. Cyber Command, for the Department, for the Nation. And so when we look across what Cyber Command and NSA [National Security Agency] are responsible for, in Cyber Command we have now grown an academic network to allow us to partner with universities across the country. So we have right now around 120 universities; in the National Security Agency, around 430. Both of those provide a really foundational opportunity for us to participate with our academic institutions on growing cyber curriculum and also working with a number of research institutions to be able to allow us to recruit that talent.

So when we think about it internally to our organizations, that is how we maintain our partnership, growing relationships with historically black colleges and universities, and also looking at universities like University of Texas at San Antonio, that has a large number of first-generation Americans and Hispanic-Latino population. Drawing talent from across the country to be able to ensure that we have the highest qualified workforce.

Mr. KHANNA. And do you need more flexibility from Congress? Because I have heard mixed things in terms of you want someone to come for 3 years, 4 years, and then they want to go on to the private sector. Are you able to do that? Are you able to have flexibility if you want to recruit someone who doesn't have a college degree and is talented or wants to do a few years? Or do you need more flexibility in the hiring?

General HAUGH. So last year one of the studies that we executed was under Section 1502, and it was about readiness. And I am required each year to provide a report on service readiness. In that report, we identified five provisions that were all around personnel and administrative policies. So what we are really looking for is we are seeing good things happening in each of the services. We would like them all to adapt each others' best practice.

So as you identified in this NDAA, Section 1535 was to begin to drive those authorities across the Department. And I think that would be an example of a step where we want to continue to provide updates on which types of provisions would help and then we work together with the services to be able to enact those provisions.

Mr. KHANNA. Ms. Manning, I don't know if you have any comments or thoughts on how we recruit more talent into our military.

Ms. MANNING. I would say, first of all, I really applaud the efforts that are underway to tackle this issue. It is a real challenge across government in terms of how you recruit and retain top talent to support our ongoing efforts, and really building out the workforce that is necessary for us to be able to accomplish our operational missions.

So I think, in addition to what we are dealing with in the Department, I think looking at sharing best practices across other departments and agencies will help generate new ideas in terms of what more we can do as a government to ensure that we are bringing people in to be able to serve our missions.

Mr. KHANNA. One of the things—and you don't have to answer it now, but I have just been told that there are some restrictions on people being able to be hired only for a few years, that that is hard to do because of civil service protections. I don't know if that is the case or not, but I just—I didn't know if Congress needs to act in any way to simplify that.

General HAUGH. What I would expect you are referring to is our ability to have people leave and come back.

Mr. KHANNA. Right.

General HAUGH. And those are areas that I think we have got to work internally within the Department in terms of how we leverage the policies that we already have, but I think that is an area that we should be continuing to explore, that if somebody leaves and goes to industry, how do we bring that expertise back into our force, not as if they are a new hire but they are returning expert back into the Department.

Mr. KHANNA. Thank you.

Mr. GALLAGHER. Mr. Gaetz.

Mr. GAETZ. Ms. Manning, I think you are totally right when you say that China is prepositioning capabilities in advance of some deployment of them. Is one way China does that by having U.S.-based technology platforms that they own or control in order to preposition for their cyber capability?

Ms. MANNING. Thank you for your question. You know, as I said, PRC is really our pacing challenge. And, as you note, they are using malicious cyber activity to counter U.S. conventional military power and to degrade the combat capability of the Joint Force. And we need to ensure that we are employing both defensive and offen-

sive capabilities to strengthen our deterrence and gain our advantage.

I defer to General Haugh for more of the details when it comes to how we are operating.

Mr. GAETZ. Yeah. I am really interested in the defensive part vis-a-vis like what China might be doing with technology platforms in the United States. Do you have anything to add on that, General?

General HAUGH. So I think the area where we have seen specific action that has concerned us is hacking activity at our critical infrastructure and at Guam. I think those are specific examples. In use of technology within the United States, having Huawei presence, and things like that, is risk. We—

Mr. GAETZ. Right. So that is what I want to get into, because I agree. The hacking is sort of like if they are breaking into your house, but the Huawei example you give is more like inviting them in the front door.

Have either of you heard of this company called Tutor.com? All right. So this is a technology platform that is owned by Chinese nationals through the Primavera Holdings Limited company, and it is principally used by DODEA [Department of Defense Education Activity], by the Department of Defense's education system, for military connected families.

If you had a technology platform that was being used specifically by military families owned by Chinese nationals, would that raise any red flags based on what you are talking about regarding the need to be well-resilient to that prepositioning that Ms. Manning discussed?

General HAUGH. I think we want to dive deeper and ensure that we are not bringing risk in, by whomever we partner with and whatever company.

Mr. GAETZ. Yeah. No, I would just encourage it, because this one sort of—I mean, I know how much you care about resilience, particularly with our service members and their families. We all know that they are targets oftentimes. And so if we are inviting the Chinese in the front door here, I just would advise you to look at that.

And I would draw your attention to the fact that Manny Diaz, the Commissioner of Education in the State of Florida, has advised superintendents of schools and charter schools to discontinue the use of this technology. And even after the State of Florida Secretary of Education made that pronouncement based on these ties, the Department of Defense education system continued to offer that platform to students of military connected families in Florida and elsewhere.

So shifting gears just briefly to this concept of the cyber force, I want to draw a finer point on what Mr. Khanna was saying about recruitment. I have noticed anecdotally at our academy nights that we have in our district that we get a lot of students that are real interested in going to the academies, and they are fired up about space force.

And I never really understood how a focused mission set like that could really ignite a great deal of interest. And do you think that we could get the same type of positive effect with the cyber force to recruit specific people for a specific domain? General?

General HAUGH. So I think from our standpoint what we have done is we have really focused on, what are the services doing? How are they doing in terms of recruiting? One of the——

Mr. GAETZ. They are not doing great.

General HAUGH. So what they have done, Congressman, is in specific areas, particularly as I look—the area we focused on has been the Navy, and as we have looked at where the Navy's readiness has been. This past year, the Navy got 100 percent of their cyber warfare technicians in terms of their recruiting numbers. That shows me the services can do it, and that a focused effort and continue and sustain that they will be able to meet some of those marks.

Mr. GAETZ. I am open-minded. I think Chairman Gallagher made some good points.

And, Mr. Chairman, before my time concludes, I wanted to thank you for your outstanding service as chairman of our subcommittee, your great work on the House Armed Services Committee, and in the House more broadly. It has certainly been to the country's benefit, and it has been to my personal benefit to sit next to you for 7 years, 8 years, and to learn a great deal from you along the way.

And I know many of our committee members feel the same, that the thoughtfulness you brought to the position has certainly been a great—been a great benefit to all of us. So greatly appreciate it and yield back.

Mr. KHANNA. Mr. Chairman, if I could speak out of order, because I didn't know this was your last meeting, and I don't know if there is an objection. But I just want to say from the Democratic side that it has really been a pleasure working with you, and you have displayed a patriotism and bipartisanship on this committee that I think has been a model for what leadership looks like. Even when we have disagreed, I have never questioned that you have put the country's interests first. And I know that this isn't going to be the last of your public service. And you certainly have someone who is an admirer on this side, and I think many of my colleagues feel the same.

Mr. GALLAGHER. I very much appreciate it.

Mr. Ryan.

Mr. RYAN. All right. Well, I guess I am not allowed to say nice things, so——

[Laughter.]

Mr. RYAN. Thank you, Mr. Chair. I will leave it at that, on many levels.

And thank you both for being here. I want to build on some of the different directions some of my colleagues were taking, particularly honing in on as we continue to, to everyone's credit, across the board develop more mature and robust and sort of broader cyber capability, I want to push and get your thoughts, General, on kind of that—what is that right intersection point between CYBERCOM services, COCOMs [combatant commands]?

I know that is a very broad question, so maybe to hone it a little bit, can you—let's talk about—let's look actually at the EUCOM [U.S. European Command] AOR [area of responsibility], for example, just as—in theory. How is that playing out right now? Where do you see the future going in terms of, as we build more capa-

bility, how—what is the right handoff point to COCOMs and services? Does that make sense?

General HAUGH. It does. And what I would first start with is, where are we today, in terms of now the authorities that you have given us and the Department has given U.S. Cyber Command? For the real general standup of U.S. Cyber Command, our goal has been to become SOCOM-like [U.S. Special Operations Command], to have service-like authorities.

Two weeks ago when the appropriation passed, that is the first time that we have now had service-like authorities to do budget, to do acquisition, to set the training standards for the Department. So now what we really want to be graded on is, what is our ability to generate new capability?

So, as things emerge, so today our partnership with EUCOM is really strong, and I was the component to EUCOM as the Air Force Cyber Commander and the 16th Air Force Commander at the outset of Russia-Ukraine. And so that partnership is really about them driving priorities in that theater, and then how we leverage each of our components to be able to respond to that, to be able to do defensive activities at their priority, but also to be able to generate options that give a number of things to the secretary and to the EUCOM commander that allow us to consider how we would impose costs based off of their guidance and direction.

I think it has worked well. I think the area that we need to be able to accelerate is capability development. And how we use our budget control and our authorities to generate and acquisition, we should be able to develop things faster than anybody else in the Department. The only thing we are developing is code. How do we do that faster? How do we get it in the hands of our cyber mission force faster?

Mr. RYAN. And you see that primarily happening or the large preponderance of it happening at need essentially rather than out there. Where do you—where do you see that?

General HAUGH. We see increasingly that that would be a balance. We will drive the requirement, we will drive the overall acquisition oversight, and the dollars, but we will also partner with the services. It will just look different. Whereas, before the services would be able to do—were doing that in support of their own forces they presented, which was very disconnected from operations.

We are now going to be able to drive that, and we have got good service partnerships with their program offices and with their acquisition force. So we need to be able to move faster, and we need to be able to recast those relationships that are more responsive.

Mr. RYAN. And last follow up on this thread. So am I hearing you right that the general direction, though, is more capability at the CYBERCOM command level to push more, you know, technical capabilities out there? Do you have the—do you have enough sort of people and capability at your level to do that? Like do you see the direction—do we have the pace that we need? Do you have the resources you need to speed that up?

General HAUGH. So from our perspective, the Department has asked us to be the integrator of the joint cyber warfighting architecture. That is the—those are the platforms and capabilities that

Cyber Command fights from. So for that now, we have got to be able to drive that with our authorities.

Our team that we have from an acquisition perspective I am very confident in. They are small. We have now been given more resources. We have to hire quickly, and we have to use the authorities that Congress has given us to be able to hire data scientists under what we previously knew as the Section 1708 authority. We have now started to hire. We have got the policy in place. So we have got to use all of those tools to really accelerate our acquisition team to be able to meet those objectives.

Mr. RYAN. I only have 40 seconds, but at the—as you look 10 years ahead, or 20 even, in terms of the quality of the American, essentially, you are getting to show up, what more do we need to do at the sort of community college level, high school level? I know that is a big question for 30 seconds, but—

General HAUGH. So I think we have an opportunity. We have expertise, and we have got partnerships across the—really, the cadre of higher institutions that are really focused on cyber. We can help influence that curriculum. How do we accelerate the curriculum in a way that allows them to adopt and then to be able to make it more available, particularly as technology changes? Because I think what we find when we receive somebody today, they have a good foundation, but they are not necessarily current today.

Mr. RYAN. Thank you. I yield back, Mr. Chair.

Mr. GALLAGHER. Dr. McCormick.

Dr. MCCORMICK. Thank you, Mr. Chair. And at the risk of being gavelled out for being out of order in this—in this era of politics where people are vilified for agreeing and vilified for dissenting, Mr. Chair, it has been an honor to serve with you, my fellow Marine. Let me just summarize by saying you can be my wingman anytime. I am the Top Gun class, so I can say that.

Considering we are at war, basically cyber war right now, and our adversaries are attacking us regularly, almost momentarily, around the clock, 24 hours a day, and how AI [artificial intelligence] will affect that into the future and accelerate that process, a lot of times the perception at least is that we are always on the defense.

I was hoping, General, you could actually address that over the last 2 years the new concept, such as persistent engagement. Hunt forward and defend forward have started to dominate the conversation, and I was hoping you could elaborate on how the wider concepts are distinct from each other as we go forward.

General HAUGH. Congressman, thank you for the question. So, first, as we think about campaigning against any one of those adversaries that are targeting either our Nation or the Department, we really think of it through three lenses. First, how do we generate insights? How do we understand what is underway? How do we communicate that to the broadest audience possible? How do we enable defense? That is enabling industry, it is enabling the Department, it is enabling our foreign partners. And then, what are our options to impose costs?

Some of those are how we use our defensive force, and then others are how we partner across the interagency, and then how we generate options that allow us to contest in cyberspace. So I think

from our perspective we want to be able to bring a full menu of not only defensive activities but those things that we can do from both the interagency and from the Department to impose costs.

Dr. MCCORMICK. Is there anything that we can do to keep you from being inhibited from doing what you need to do to be optimized going forward using AI and other weapons that we have to be not just posturing defensively but also being proactive?

General HAUGH. So I think what you have done is you have empowered us in a number of different ways in terms of how we have brought together our acquisition force and how we have brought together our authorities. We will identify areas throughout this year, as we begin to use those authorities, that I suspect you will start to see in budget requests for fiscal year 2026.

We are going to learn a lot with the establishment of our AI task force. We completed an AI roadmap last year, and that lays out for us the technologies that we want to begin to experiment with and pilot and introduce to our force. Those will be areas that I would expect you are going to see from us in the future.

Dr. MCCORMICK. That is great. With that said, now that we looked—this was brought up, interestingly enough, by our chair, as far as the integrated Cyber Command versus the individual departments. I have had plenty of people here testify saying, well, we like—can I keep this in columns, because each service has its own specific requirements.

But as AI continues to be a problem in integration, whether it be on weapons systems, information collecting, dissemination of information, the way it needs to be integrated throughout purple force, if you will, my concern is that we will have difficulties integrating even different weapons systems, let alone the comprehensive battlefield, like when you talk about purple assets, whether it be electronic jamming or information gathering.

I am just wondering, is there a compromise in there that we could come to in information sharing? Which is already the biggest problem we have in the military anyway. It is just kind of our Achilles heel, whether it be through COMs [commands] or just getting the right information to the right people in the right way. That is my biggest concern. If we don't have a Cyber Command, how do we do that in an efficient way?

General HAUGH. So what I would—the way that I would—the way that I think the Department looks at it, the deputy secretary has really empowered the CDAO [Chief Digital and Artificial Intelligence Office] to set our data standards, and to do that across the Department. And so when I look at our teammates that we have in the DOD CIO [Chief Information Office], in CDAO, how do we enable their ability to go faster in some of those data standards?

And I think we have a role to play in that, and I think we can help and assist, not only in how we set some of those standards but how we think about defense of each of these activities from a cyber perspective from the outset as we begin to introduce some of those new technologies.

Dr. MCCORMICK. Okay. I just—for the record, you can see a lot of Congressmen are concerned about this integration process. China has a huge advantage in this one area. They have one command structure, one government. They all agree on each other be-

cause it is kind of a monopolistic government, and it is going to be a lot easier for them to integrate AI throughout their weapons systems. The way they do digital technologies, it is a lot less distractions. They have a lot more focality. And I think if we get outpaced in the AI arena, we are in big, big trouble. So I hope we do a good job on that.

Thank you. With that, I yield.

Mr. GALLAGHER. Mr. Moulton.

Mr. MOULTON. Thank you, Mr. Chairman. And thank you very much for being here.

A couple weeks ago the Foundation for Defense of Democracies think-tank issued a report calling for a separate cyber force. And I suspect you have read this. I know this is not a new topic. It is something that I have discussed myself over the years.

And I was curious—I mean, basically, the main argument of the report is that because the individual services each run their own recruitment, training, and promotion systems for their cyber operations, those who get sent to U.S. Cyber Command have inconsistent knowledge and qualifying experience.

So, General, how have these inconsistencies across the services impacted the effectiveness of U.S. Cyber Command in executing its mission?

General HAUGH. So, Congressman, first, if I could address the study, one of the areas that I do think that as we go through this year the 1533 study, and we evaluate all of the options available for force generation, we certainly are going to look really closely at, what are the implications of a cyber service? We will evaluate that.

One of the other responsibilities that is in both our unified command plan and in the law is that I am responsible to evaluate the overall health of the DOD cyber workforce. So I am responsible to do that in plain English both to the Secretary of Defense and back to Congress.

So I think from our perspective, those reports have allowed us to identify where are areas that the services could improve. And in doing so, it has also allowed us to build a partnership with the services on how do we work together to improve the readiness? Because I think what areas we had seen in the past was not necessarily from the recruiting perspective but more so from the assignment and retention.

And Congress has given us a number of authorities to the Department that allow for retention incentives. What we were seeing was the services implement those differently, and so what we are encouraging, and what we did in our 1502 report last year was to ask for some specific authorities that encouraged our ability for assignment policies and personnel policies to ensure that those trained individuals stay in our force. And we have seen the services respond to those requests.

So we want to be able to lock those in and then continue to work on other areas that will improve readiness within the force.

Mr. MOULTON. Do you feel that you are doing enough to use the authorities that Congress has given you?

General HAUGH. So I think now that we have budget control authority that we received last month, that now gives us a new series of options that will allow us to drive our priorities in training, in

readiness. We are responsible for the advanced training of the Department's cyber force. How we use those dollars in many ways will determine our readiness and our proficiency.

Mr. MOULTON. I would like to ask just a couple of questions about deterrence. Deterrence is obviously important writ large, but of course when we look at a China attack on Taiwan, we want to deter that from happening in the first place. Deterrence is tough in the cyber world because we worry about giving up our capabilities when we use them.

How is your thinking about this evolving? And how do you think—I would love to hear, General, a couple of comments.

And then, Ms. Manning, how do you think about this in the integrated deterrence environment?

General, perhaps we could start with you. Just how—with cyber force, how do you think about deterrence?

General HAUGH. So from a Cyber Command perspective, what we really think about in integrated deterrence are, who can we bring that is a partner that will allow us to be able to have the outcome we are trying to achieve? And for us, those partnerships look different than in some of the other domains.

When we think about how—the role that industry plays in terms of both creating the domain and also being the ones with our own sensors that are global in nature, how do we partner with industry? How do we partner with our foreign allies and partners that either bring capability or have the same common thread? How do we partner with our fellow combatant commanders as they think about cyber security and defense? And how do we integrate capabilities together to be able to have options?

So I think for us we have a unique set of partners, and we have got to be able to use our authorities in how we defend forward and do it every single day.

Mr. MOULTON. Ms. Manning, how are you thinking about working with your counterparts in other agencies to fulfill this goal of integrated deterrence?

Ms. MANNING. Thank you for your question, Congressman. We really do see cyber deterrence, as you mentioned, as part of overall integrated deterrence, in thinking about integrating across the Department, across domains, across the interagency, and also with allies and partners in those private-public partnerships that General Haugh mentioned.

And it is important that we work together with our interagency partners, with our partners in industry, and with our allies and partners to really look at ways that we can deny adversaries the benefit of cyber attack by, one, being able to provide indications and warnings of threats to benefit our interagency partners, and then also by imposing consequences on our adversaries by disrupting their operations.

Mr. MOULTON. Thank you, Mr. Chairman.

Mr. GALLAGHER. Thank you. I should note the Section 1533 study that I referenced earlier was, I believe, Mr. Moulton's amendment. So he deserves credit for provoking and stimulating the debate that led to the report he referenced, and so I thank him for that.

Mr. Fallon is recognized.

Mr. FALLON. Thank you, Mr. Chairman, and thank you for your service to the country. I am sorry to see you go. But as—to quote the immortal words of Dr. Seuss, don't cry because it is over; smile because it happened.

Last November, the North Texas Municipal Water District got hacked, and it was a domestic—it was a domestic attack, but, nonetheless—and they didn't shut it down, but they showed that they could have. And it reminded me of JBS and Colonial Pipeline.

And, General, I wanted to ask you, what have we learned? Because that is the greatest fear we all have is that these critical areas—water, electricity, energy, fuel. What have we learned from those attacks that we can employ within the Defense Department?

General HAUGH. So I will give you a couple different things, Congressman. One is this is an area that we have clearly identified that the PRC is targeting. So this wasn't in this case, but we know that it is an area they are targeting. So from a national readiness perspective, we have to consider that.

The other thing we think about is, what does it look like for defense critical infrastructure? Those things that are the nexus between our private infrastructure and those things the Department would rely upon if we were mobilizing. So that is a partnership with NORTHCOM [U.S. Northern Command], and it is a partnership with Homeland Security.

I think those are areas that within the Department we have now focused, how do we think about that nexus, and what will it mean for the Department from a cyber security standpoint? So I think we have now been applying some of those lessons. We are going to have to continue to scale as we think about it within the Department.

Mr. FALLON. And then, you know, with—you mentioned that CCP [Chinese Communist Party] and, like, Volt Typhoon comes to mind, there is no doubt that they are actively probing, of course. Can you talk about the work that you are doing with industry partners? Because, you know, chain, meet weakest link. If we have got some of our partners buttoned up and secure as a uniformed service, or even along the DOD, but a private company that is working with us isn't, it doesn't get us anywhere.

So can you talk to us about what we are doing to enhance particularly the cyber security of our partners?

General HAUGH. Yes, Congressman. Both Congress and the Department have given Cyber Command and NSA authorities to work with our Defense Industrial Base. And that information-sharing component has now allowed us to establish over 1,000 partnerships, and that allows us to exchange information, it allows us to do it in real time at an unclassified level, so that we can make industry aware of those threats.

As we think about those partnerships, now DOD CIO has also funded additional activities that allow us to provide services to the Defense Industrial Base—protective DNS [Domain Name System]—so that they have a service that would make it more difficult for a redirection attack or a spear phishing attack informed by NSA's knowledge.

The other things we have been doing are scanning of various elements of the Defense Industrial Base. We provide them a scan. We

tell them what vulnerabilities we see and allow them to correct those vulnerabilities themselves. We are going to continue to look at what other services we can provide, but we are also looking at how can we extend those partnerships to a broader number that would ensure that we are covering the highest priority things that support the Department.

Mr. FALLON. Thank you. And then, you know, when people come into our offices, they are all dying for labor. It doesn't matter what industry it is. I ask them, "Do you have—you know, do you have job openings?" and they are all crying for labor, so—and particularly skilled labor even more so.

So I wanted to ask maybe Ms. Manning as well, what can we do, if anything, do we need to do? I remember being a junior officer and the doctors got paid more because, you know, that is just the market, right? You want to—you want to have those medical doctors stay on after maybe they owe some time after getting—going through medical school.

But in particularly this field, it is just a high demand, and it—they make quite a bit of money. Do we—is there incentive pay for folks in this service? And does it need to—do we need to ratchet it up? I just want to kick that to both of you.

Ms. MANNING. You know, I think at this point it is important that we consider all different ideas of how we can recruit and retain top talent. I think incentives are one tool that we have in our toolkit. I think also, though, there is a sense of mission that comes with doing the work in the Department.

And so thinking about how we can make people feel really connected to the mission itself is another thing that we can think about. But I think really understanding what is it that is motivating people to come to these jobs, what is allowing them to sustain careers in government long term, and I think pay incentives are one of the tools we have at our disposal.

Mr. FALLON. I just don't want the canyon to be this big. You know, if it is 300-grand in the private market, and it is 100-grand here, that is just too big of a canyon, even if you are really rewarded, if we can close it. That is kind of my point.

Thank you. Mr. Chairman, I yield back.

Mr. GALLAGHER. Mr. Luttrell.

Mr. LUTTRELL. Thank you, Mr. Chairman.

General, in December 2022, SECDEF [Secretary of Defense] officially elevated CYBERCOM's offensive arm, the Cyber National Mission Force, to a sub-unified command. The logic was that it would provide greater enabling resources for this critical mission set. With how much adversary activity we have witnessed against DOD networks, it would appear that your defensive arm, Joint Forces Headquarters, could similarly benefit.

Could you share your opinion?

General HAUGH. Thank you, Congressman. So when we stood up—when we elevated the Cyber National Mission Force, it was at a point, so we now—that is about a third of our force, and with a very distinct headquarters and assigned forces. That has—now I think was absolutely the right thing for us to do, that we are allowing it to create an identity, we are allowing it to grow its own staff

to expand its planning, and then—and other capability development. I think we are seeing benefit from that.

This is an area that we are going to look at in the 1533 study, which is, as we start to think about—or, actually, the 1537 study that you have asked us to do looking at our headquarters. What is the right way to position the Joint Force Headquarters DODIN [Department of Defense information networks] in terms of the right resources and authorities to make sure that it has the capacity to really set the globe? That is the mission we have given them.

When we have a crisis, we want them to set the globe. So I think it is an area that we are certainly going to evaluate, and it does look different as a headquarters, also in terms of assigned forces, but it is something that we will definitely be looking at.

Mr. LUTTRELL. Thank you.

Ms. Manning, I apologize for walking on Mr. Fallon's questions. To expand or to create an expansiveness of talent, we wanted to reach out to academics—academia and institutes of higher performance, correct? Are we doing that, from your—in your opinion?

I have universities in my district, and then of course, as I travel the state and the country, I have these discussions when it comes to cyber risk, cyber threat, cyberspace, artificial intelligence, machine learning, and how it seems like we are missing the rising wave, because our brilliant minds are traveling elsewhere. Are we creating effective narrative from your position in order to share that with the youth and say, "Hey"—and I say "youth," but our next generation of computational mathematicians.

Ms. MANNING. I think there are two aspects to this. I think one is making folks see a career in government as something that they want to pursue, and they see building the skills in cyber and in other fields as something where they can have a unique role in terms of defending our national security interests by having jobs you can really only do when you are in government, so—

Mr. LUTTRELL. So how do we make working for the government sound cool?

Ms. MANNING. I think that is a really important point, and I think also beyond just making it sound cool, how do you have the—

Mr. LUTTRELL. For lack of a better term, I am sorry, I should have stated that better.

Ms. MANNING. No. I think, you know, it needs to be relatable, and we also don't need the mechanisms to bring people into government. So looking at different tools like the cyber accepted service, looking at the presidential management tool, fellowship, looking at different scholarships and opportunities, I think all of this should be on the table, so that we can give folks the opportunity not only to want to serve in government but to be able to have the mechanisms to come in and be able to be a part of our team.

Mr. LUTTRELL. Are we looking at having them serve in the various branches of armed services or just government in general? Because, as we know, we are having trouble recruiting the bodies for those platforms. Is it both, in between, or is it just something we are trying to cast that wide net and fill all of the—all of the silos?

Ms. MANNING. I would defer to the team who is responsible for personnel and readiness in terms of the overall policy.

Mr. LUTTRELL. Oh, that is a great shift.

Ms. MANNING. But I think there are opportunities, both within the command, within the services, or for individuals to come in and to serve.

Mr. LUTTRELL. General, have you got something on that one?

General HAUGH. So what I would give you is, what do we see that are things that are pretty exciting that are really looking at high schools and middle schools? I just attended the finals of CyberPatriot, 5,000 schools across the country where they are doing cyber competitions in middle school and in high school and in ROTC [Reserve Officers' Training Corps] programs.

Those are the types of things that we want to be able to do as early—we would like to see being done as early as possible, so that we are really trying to capture people and what it looks like to be—that can be both cool and really impactful things for our Nation. I think—

Mr. LUTTRELL. They seem like they have a willingness to put a uniform on?

General HAUGH. I think what we have seen is they have done a really nice job of bringing people towards the technology, and then it is our job to be able to have opportunities with the ROTC programs that are in high school and also to be able to reach out and be able to explain, what would you do if you came and worked with us, either as a civilian or in the military? That is our story that we have got to tell. Yes, sir.

Mr. LUTTRELL. Thank you, Mr. Chairman.

Mr. GALLAGHER. Thank you. Does any other member have a follow-up question?

Okay. The FDD [Foundation for Defense of Democracies]— we are going to have a classified session after this. But I think the FDD report that you have heard referenced numerous times here— again, I think—I mean, I am biased because I worked with a lot of these people in the Cyberspace Solarium Commission. I will admit that. But I think what is most compelling in it is the testimony from active duty, ranging from company grade to general grade officers.

And I would like to read one statement from a Marine Corps captain, and all wisdom emanates from Marine Corps captains, as Mr. Moulton and I know quite well.

“Leading in the cyberspace domain demands technical competency that cannot be taught in a 12-month schoolhouse alone. One of my worst professional experiences involved working underneath a woefully unprepared commander with a degree in culinary arts. Under no circumstance would a cyber officer be asked to lead a squadron of aircraft, and that the opposite is often true.”

That is just one of many quotes in the report that I think are worth reading. And, again, I am not biasing the outcome of the study you guys are going to do or an independent study, but I just think it is fair to say at this point that the status quo is not getting the job done. So we are asking you to take a hard look at this problem and work in partnership with us to come up with a better model.

As was referenced by some of my colleagues, we have given so many authorities to DOD in the 8 years I have been on this com-

mittee, and it has all been well intentioned. It just seems like it is not adding up or producing the outcome we want.

And so I know you are both relatively new to your respective jobs, and they are critically important jobs, and our commitment is to work with you to get this right, because the safety of our country and our citizens are quite literally hanging in the balance. And so we appreciate your time today. We look forward to the classified session.

And, finally, since he was not here when I said nice things about him, I just want to reiterate how much of a pleasure it has been to work with Ranking Member Ro Khanna, not just on this committee but on many issues. One of my fondest memories is the op-ed we did on congressional reform together when we were impetuous freshman members of Congress.

Mr. KHANNA. Still no reform.

[Laughter.]

Mr. GALLAGHER. Still no reform. Yeah. My biggest failure. Term limits didn't happen. We went to the White House together to talk about that.

But, Ro, you have always been incredibly, obviously, smart and independent-minded, but you have a bias for action that I admire, that I think is rare among people in public service, and I also appreciate your sense of humor and that you take the mission, but not yourself, too seriously.

So thank you for your productive partnership. Appreciate that.

With that, the open hearing is adjourned, and we will move to a classified session.

[Whereupon, at 4:30 p.m., the subcommittee was adjourned.]

A P P E N D I X

APRIL 10, 2024

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

APRIL 10, 2024

Opening Statement (As Prepared) Ranking Member Ro Khanna

*Cyber, Information Technologies, and Innovation Subcommittee Hearing:
"Cyber in an Era of Persistent Engagement"*

April 10, 2024

Thank you, Mr. Chairman, and thank you for all your hard work and leadership this Congress. It's been a pleasure to work alongside you on this subcommittee and throughout our time together in Congress, and you will be sorely missed. I know you will greatly miss this work.

To our witnesses, thank you for appearing before the committee today. As the Chairman noted, this is your inaugural visit to this subcommittee, and we look forward to working with both of you in your new roles.

Ms. Manning, while your role as an Assistant Secretary of Defense is now less than a month old, you've inherited a number of ongoing challenges. I look forward to hearing more not just about the organization and intra-Department relationships that will evolve with your new role, but about the ongoing efforts contained within the Fiscal Year 2025 budget request that now fall to a greater or lesser extent under your purview. In particular, I hope to hear more about the forthcoming Cyber Posture Review, the implementation of the DoD Cyber Strategy, and the status of the numerous other Congressionally-directed studies and reports that impact the future of the DoD cyber enterprise.

General Haugh, it's good to see you again, and I'd especially like to thank to the men and women of U.S. Cyber Command that you represent here today. I look forward to exploring the numerous issues under your purview, and in particular I hope to hear more about CYBERCOM 2.0 and the implementation of enhanced budget control.

My district is home to some of the most innovative companies in the world, and many of them are key players in cyberspace and digital innovation. Their expertise is and will continue to be essential in maintaining the United States' technological edge. Too often, though, the Department of Defense is its own worst enemy when it comes to fully harnessing the power of the private sector. I hope to hear from both of you about what more the Department of Defense and U.S. Cyber Command can do to accelerate iteration and adoption for cyber-

I know both of you are also focused on addressing our workforce challenges. While progress has been made and momentum is building across the Department, I hope we can explore today what further efforts may be needed.

Thank you again to our witnesses, and I look forward to today's discussion. I yield back.

STATEMENT OF
MS. ASHLEY MANNING
PERFORMING THE DUTIES OF ASSISTANT SECRETARY OF DEFENSE FOR CYBER
POLICY
TESTIMONY BEFORE THE
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON CYBERSECURITY, INNOVATIVE TECHNOLOGIES, AND
INFORMATION SYSTEMS
APRIL 10, 2024

Introduction

Chairman Gallagher, Ranking Member Khanna, and distinguished members of the Committee, thank you for inviting me to testify on the Department of Defense's cyber posture and the advancements we continue to make operationalizing the Department's priorities in cyberspace. It is an honor to appear alongside General Haugh, the Commander of U.S. Cyber Command (USCYBERCOM), who brings a breadth of experience to this position as we strive to keep pace with the rapidly evolving threat environment in cyberspace.

In my role Performing the Duties of Assistant Secretary of Defense for Cyber Policy, I am committed to providing overall supervision of the Department's policy for cyber, advancing the Department's strategic approach to cyberspace, and ensuring our readiness to counter emerging cyber threats. Mr. Chairman, I look forward to working with this Committee through my newly established office to further these objectives.

I come to this role as a career civilian with almost twenty years of service in the Department of Defense. I have had the privilege of working across a wide range of regional and functional issues including serving as Acting Deputy Assistant Secretary of Defense for the Middle East and the Principal Director for Plans and Posture in the Office of the Under Secretary of Defense for Policy. I also served as an exchange officer at the UK Ministry of Defence, where I was the Deputy Head of Strategy and oversaw the development of Defence's contribution to the UK Integrated Review strategy. In each of these roles, I have witnessed the cross-cutting role cyber plays in the defense of our Nation and our Allies and partners.

The President has nominated Dr. Michael Sulmeyer as the ASD for Cyber Policy. Should he be confirmed, I look forward to serving as the Principal Deputy Assistant Secretary of Defense (PDASD) for Cyber Policy.

Security Environment

Cyberspace serves as a cornerstone of global connectivity, communication, and innovation. It has revolutionized industries, bolstered our national prosperity, and enhanced the agility of our Joint Force. However, it also exposes us to diverse threats from malicious cyber actors seeking to exploit this interconnectedness for their own gain. Defending against these threats, both domestically and abroad, is paramount for the Department of Defense.

The People's Republic of China

Our National Defense Strategy (NDS) makes clear that the People's Republic of China (PRC) remains an enduring cyber threat and the Department's pacing challenge in cyberspace, as the PRC continues to target U.S. networks in prolonged campaigns of espionage and to pre-position its cyber forces for future operations. The PRC views cyber and information dominance as critical advantages, spurring continued investment in the technology sector and cyber forces. A key component of the PRC's strategy includes substantial investment in cyber espionage efforts, such as stealing intellectual property, research, and sensitive information from American citizens. This steady drain of sensitive U.S. information over time has the potential to erode advancements in U.S. military capabilities and the Joint Force's ability to project power.

In addition, a group of PRC cyber actors known as "Volt Typhoon" were first observed in mid-2023 pre-positioned on multiple critical infrastructure networks for potential disruptive or destructive cyberspace attacks in the event of a major crisis with the United States. These cyber threat actors leverage a technique referred to as "living off the land," which allows them to blend in with normal system and network activities, evading detection and making it very difficult to identify "Volt Typhoon" actors. These potentially destructive operations are part of a broader cyber campaign driven by PRC national and military objectives, one the Department is prepared

to meet to preserve the ability of the Joint Force to fight and prevail in a contested cyberspace environment.

The PRC views information as a tool to be tightly controlled in service of consolidated authority. This is evident in PRC vulnerability disclosure regulations that mandate companies to report software vulnerabilities to government authorities within forty-eight hours of discovery, expanding the government's mass collection of software vulnerabilities. These requirements continue to exacerbate the challenge PRC cyberespionage and pre-positioning poses to the United States and our partners, because they provide PRC offensive cyber forces a virtual warehouse of cyber weapons that can be leveraged with impunity by the PRC government. Due to the dynamic nature of the cyberspace operating environment and the constant discovery and patching of software vulnerabilities, maintaining a new and robust list of vulnerabilities provides a distinct advantage.

Russia

Russia remains an acute threat to the United States and our Allies and partners as it continues to leverage cyberspace to target critical infrastructure networks and enable its malign influence operations. Russia maintains concurrent cyber campaigns targeting potential victims in the United States and North Atlantic Treaty Organization (NATO) nations and considers maintaining an ability to disrupt and degrade critical infrastructure Industrial Control Systems as a priority. Russia continues waging its war on the people of Ukraine, including by employing a range of cyber capabilities to disrupt Ukrainian military operations and erode political will for Ukraine's defense. Last year, Russian-linked cyber actors were observed spying on Android devices used by the Ukrainian military, providing an advantage to Russian military forces responding to Ukrainian military maneuvers. This past December, Ukraine was also the victim

of a malicious cyber activity against its largest telecommunications provider, impacting millions of civilian subscribers in Ukraine. The ongoing unprovoked further invasion of Ukraine serves as a stark reminder of Russia's willingness to employ cyber capabilities to disrupt defensive military operations and sow discord. Another concerning trend is Russia's cooperation with Iran on cyber. For example, in March 2023, Russia sent Iran digital surveillance software, and Tehran is seeking more assistance from Russia.

Other Persistent Threats

Following Hamas's attack against Israel on October 7th of last year, Iran has exploited cyberspace to create additional disruptions and challenges in Israel. Iran recently used an online persona to claim credit for malicious cyber activity targeting Israeli-made devices commonly used in the water and wastewater sectors, impacting multiple victims in the United States. While many of these malicious cyberspace activities have been relatively limited in their impact, the ability of both state and non-state actors to act against Israel in the immediate aftermath of the Hamas attack is a reminder of what to expect in future conflicts.

The Democratic People's Republic of Korea's (DPRK) cyber actors remain intent on stealing and acquiring cryptocurrency to generate revenue for the regime's weapons of mass destruction and ballistic missile programs. The DPRK was responsible for the theft of hundreds of millions of dollars in cryptocurrency last year and continues to seek opportunities to leverage commercial firms to facilitate its laundering of stolen funds.

Additionally, the United States continues to face the still-growing threat posed by for-profit cyber criminals that target a wide array of vulnerable sectors, conducting ransomware attacks that impact the daily lives of Americans across the country. The recent ransomware attack against Change Healthcare was one of the most damaging that the United States has seen,

with both tangible and psychological impacts that influence the implicit trust Americans have in their medical providers. This type of reckless and indiscriminate targeting of civilian sectors that threaten people's lives and livelihoods is unacceptable.

2023 Defense Cyber Strategy

In response to these evolving challenges, the Department developed and the Secretary approved DoD's fourth Defense Cyber Strategy last May. This strategy, along with its unclassified summary, highlights the importance of defending forward, disrupting malicious cyber activity before it can pose risk to our Homeland, and of strengthening partnerships with Allies and partners and our Defense Industrial Base (DIB) to bolster cybersecurity efforts. The 2023 Defense Cyber Strategy builds upon years of experience conducting offensive and defensive cyberspace operations, reflecting the Department's commitment to preemptively countering cyber threats and operationalizing the priorities outlined in the 2022 National Security and Defense Strategies.

The 2023 Defense Cyber Strategy was issued at a pivotal moment as the Department prioritizes the challenges posed by technologically advanced, near-peer adversaries. The strategy draws on lessons learned from Russia's 2022 further invasion of Ukraine, which has prompted a global reconsideration of the role of cyber in conventional conflict. These events reaffirmed that war-time cyberspace operations are best understood as a complement to conventional missions rather than as a decisive standalone capability.

Russia's cyber operations in the war in Ukraine are largely consistent with the strategic miscalculations we have observed with Russia's kinetic forces. The Department does not consider this to be proof of the weakness of Russia's cyber arsenal or a failure of cyber as a tool in warfare. Rather, we assess that it is a reflection of the challenges of integrating multi-domain

operations and Ukraine's resilience, which has been reinforced by strong support from the international community and private sector partners.

Strategic Lines of Effort in Cyberspace

As we stand on the brink of what President Biden has called the "decisive decade" that will determine the shape of the strategic environment to come, DoD will seize the moment to fortify our cyber resilience and invest in our people. To that end, we continue to work across government stakeholders to execute on four lines of effort: Defend the Nation; Prepare to Fight and Win the Nation's Wars; Protect the Cyber Domain with Allies and Partners; and Build Enduring Advantages in Cyberspace.

Defend the Nation

First, we are actively campaigning in and through cyberspace to identify and mitigate cyber threats and their supporting ecosystems before they can harm the American public. In the Department, we call this "defending forward," meaning proactively disrupting malicious cyber activity to deny benefits and raise costs for adversaries. We do so by working closely with our partners in other Departments and Agencies to enable the defense of U.S. critical infrastructure and the DIB and to counter threats to military readiness. The Department has the capability to leverage offensive cyberspace operations, when necessary, with the agility and speed needed to address ever evolving foreign cyber threats in an exceptionally volatile domain. Additionally, the Department will continue to leverage operational insights gained from engagement with adversary cyber actors to bolster U.S. cyber defenses and inform the risk management approach of the Defense enterprise.

Prepare to Fight and Win the Nation's Wars

Second, the Department continues to leverage cyberspace operations to enable and empower Joint Force objectives, operating within the framework of persistent engagement to maintain constant pressure on adversaries. The Department campaigns consistently below the level of armed conflict to maintain the capability to leverage the digital domain to gain a decisive advantage in relevant conflicts. We will improve the resilience of the Department of Defense Information Network (DoDIN) and support campaign and contingency planning for joint plans and operations to reinforce both our defensive and offensive capabilities. As the Department campaigns in cyberspace for these purposes, we will develop offensive and defensive options to support the Joint Force so that it remains ready to respond rapidly across the spectrum of conflict.

Protect the Cyber Domain with Allies and Partners

Third, we are investing in our greatest asymmetric advantage – our global network of Allies and partners. Because of the interconnected nature of cyberspace, U.S. adversaries often target Allied and partner networks in order to gain access to our U.S. systems. Additionally, adversaries may test cyber tools and capabilities on partner nations, providing unique insights into adversary cyber force tactics, techniques, and procedures (TTPs) that can improve U.S. defenses against similar operations. This means that helping boost Allied and partner cybersecurity isn't just a “nice to have” – it is a national security imperative. The 2023 Defense Cyber Strategy commits to building the capacity and capability of U.S. Allies and partners in cyberspace and expanding avenues of cooperation to allow for timely information sharing and interoperability.

Hunt Forward Operations conducted by USCYBERCOM remain a key component of how the Department works with Allies and partners in cyberspace, helping to identify vulnerabilities to their networks, which in turn bolsters U.S. cyberspace defenses. We intend to continue investing in these missions, taking a collective approach to cybersecurity with the goal of frustrating the objectives of adversary cyber actors.

DoD will continue bilateral technical collaboration to identify malicious cyber activity on Allied networks while promoting responsible state behavior in accordance with international law and cyberspace norms. For example, the Department has reinforced its strong information sharing relationship with Ukraine and continues to provide defensive support to enable the resilience of Ukrainian networks. We also recognize that reinforcing responsible state behavior in cyberspace requires engagement on issues of strategic stability even with countries with whom no cyber cooperation exists in order to prevent miscalculation. Last year, the Department hosted a working level meeting with PRC defense officials to discuss the tenants of the 2023 DoD Cyber Strategy unclassified summary, in accordance with the 2014 U.S.-PRC Memorandum of Understanding on Notification of Major Military Activities Confidence Building Measure Mechanism. By promoting responsible state behavior in cyberspace, building capacity and capability among our Allies, and fostering information sharing, we strengthen our collective defenses against cyber threats.

Build Enduring Advantages in Cyberspace

Finally, the Department is pursuing institutional reforms to build enduring advantages in cyberspace. Our people are our greatest cyber asset. The Department will prioritize reforms to improve recruitment, retention, and training of the Cyberspace Operations Forces (COF) and Service-retained cyber forces. We will equip our warfighters with the essential tools and

technologies to adapt and respond continually to the emergent threats and changing technologies that we will face and prevent malicious cyber actors from achieving their objectives in and through cyberspace. Finally, the Department will prioritize necessary reforms to meet the intelligence needs of the cyberspace operations community.

Posture Review

Looking ahead, we are committed to implementing our strategy and monitoring progress through the forthcoming Cyber Posture Review in FY 2026. Since the last Cyber Posture Review was concluded in 2022, the Department has not only delivered the 2023 DoD Cyber Strategy but also has placed increasing emphasis on the quality of enterprise-wide data collection and begun streamlining data-driven analysis in collaboration with organizations such as the Chief Digital and Artificial Intelligence Office (CDAO) and the Analysis Working Group (AWG). These efforts will shape how we monitor the success of our implementation of the 2023 DoD Cyber Strategy and the readiness of the COF through meaningful metrics, improved reporting systems, and modern analysis tools. My office is currently working alongside CDAO and the AWG to develop an improved metrics and data governance structure for the next Cyber Posture Review. This enhancement will provide more accurate, relevant, and traceable analysis, enabling continuous improvement in our cyber capabilities and readiness.

Looking Forward in 2024

With an eye towards the future, we understand that the Department cannot advance its defense priorities without a ready, capable, and informed Joint Force, one prepared to operate as fluently in cyberspace as any other joint warfighting domain. To achieve this end, we will invest in our people, capabilities, and information needs to support and enable the full range of cyber activities.

People

The Department continues to view its people as the most critical driver of success in the cyberspace domain. The need to recruit, retain, develop, and reward service members and civilians with technical aptitude and skillsets becomes increasingly critical and challenging every year. In response to readiness challenges and incorporating input from Congress, the Department is continuing to execute a review and re-design of the COF. The aim of these efforts is to build a force that can gain operational advantage over our adversaries and competitors, maintain agility in conducting operations from competition to conflict, and recruit and retain the talent necessary for achieving the Nation's cyber missions.

The Department has both completed and is conducting several studies evaluating force generation, readiness, and force employment models for the COF. These reviews highlight the need to think boldly about changes to a force structure that has remained largely static since 2012 when the Cyber Mission Force was created. We are looking holistically at how to evolve the COF, focused on the mission sets of USCYBERCOM, and exploring models beyond iterative adjustments to the current approach. The Office of the Secretary of Defense, in partnership with USCYBERCOM, is refining options for the Secretary to improve how forces are presented to the Command, raise readiness levels of the force, and streamline support mechanisms to other Combatant Commands. The recommendations to the Secretary will further allow USCYBERCOM to exercise its authorities in partnership with my office.

Capabilities

I appreciate the recent budget authorities granted to USCYBERCOM and the Principal Cyber Advisor, and I look forward to supporting the Department's implementation, in partnership with General Haugh, of those authorities. Beginning in FY 2024, consistent with the

National Defense Authorization Act (NDAA) for FY 2022, the Commander of USCYBERCOM's authority to control and manage the execution of current cyber resources to man, train, equip, and operate the Cyber Mission Force is now expanded to include the planning, programming, and budgeting of future years' cyber resources. In addition, consistent with the authorities granted to the PCA in the NDAA for FY 2023, the ASD for Cyber Policy, as the PCA, will continue to review the proposed budgets of DoD components to ensure adequate resourcing for the cyber mission.

As part of the FY 2026 budget cycle, DoD released the first Department-wide Cyber Operations Programming Guidance, which will shape future investments in cyberspace operations capabilities across the FY 2026 – FY 2030 Future Years Defense Program (FYDP). This will serve as a rubric for certification of the Department's – and in particular USCYBERCOM's – future budget requests beginning in the FY 2026 cycle.

The FY 2025 Cyber Activities budget aligns with the 2022 NDS and reaffirms the Department's three enduring cyberspace missions: Defend the DoDIN, Defend the Nation, and Prepare to Fight and Win the Nation's Wars. To execute on these missions, the Department will invest in cyber capabilities supporting integrated deterrence, campaigning, and efforts to build enduring advantage including by overseeing investments across the DoD cyber community.

The Department will continue to build on the pathway laid out by the 2023 DoD Cyber Strategy and other initiatives established in past fiscal years to provide a stronger cyber posture through ongoing development, deployment, sustainment, and modernization investments in DoD cybersecurity tools and capabilities. The President's FY 2025 Budget includes \$14.5 billion for cyberspace activities which encompasses: 1) cybersecurity; 2) cyberspace operations; and, 3)

cyber research and development (R&D) activities, aligning DoD's commitment to strengthening its cyber capabilities and protecting its critical networks and systems from evolving threats.

1) Cybersecurity

The DoD Chief Information Officer (CIO) is responsible for certifying the \$7.4 billion cybersecurity portion of the President's FY 2025 Budget, and I look forward to partnering with the DoD CIO to prioritize investments in areas across the Department's information and operational technologies including weapons systems, defense critical infrastructure cybersecurity, supply chain risk management, DIB security, and key management infrastructure modernization. Additionally, DoD is building cyber resilient platforms to execute kinetic and non-kinetic missions by implementing the Strategic Cybersecurity Program, providing and assessing vulnerability mitigation plans, cryptographic modernization plans, and defensive monitoring recommendations. The Department is also transitioning to Zero Trust under the leadership of the DoD CIO, who is driving cybersecurity architecture planning, encryption modernization, and risk management of legacy Information Technology and weapon system cybersecurity.

2) Cyberspace Operations

The President's FY 2025 Budget requests \$6.4 billion for Cyberspace Operations, including nearly \$3 billion in annual budget authority for USCYBERCOM offensive and defensive cyberspace operations programs and activities, force generation and readiness, and capabilities and infrastructure directly supporting joint operations. Priority investment areas include manning, training, and equipping the CMF and advancing capable dual-use cyber ranges and testing facilities to support full spectrum multi-domain operations. The budget further prioritizes optimized equipment for hunt forward and enhanced sensing and mitigation

operations and building out the Joint Cyber Warfighting Architecture (JCWA), which encompasses many capabilities that support operations from competition through conflict. The budget prioritizes support for Indo-Pacific and European theater priorities and identifies cyberspace information collection and analysis as a critical need to enable U.S. cyber forces to prepare for and conduct offensive and defensive cyber effects operations and joint training.

3) Cyber R&D

Finally, the FY 2025 Budget requests \$629 million to support advanced R&D of new capabilities. The Cyber R&D budget will propel the Department's cyber programs forward by modernizing existing capabilities while advancing next generation tool development in support of Departmental cybersecurity and cyber operations programs. These efforts focus on developing the computing, networking, and cybersecurity technologies required to protect DoD, U.S. Government, and civilian information, infrastructure, and mission-critical systems and are crucial to accelerating efforts across the Department to implement the 2023 DoD Cyber Strategy. Over the next fiscal year, DoD will conduct further demonstrations and evaluations with warfighters, acquisition programs, and combatant commands to assess and improve prototype utility.

Information

Undergirding all of our work to develop capabilities to ensure overmatch against U.S. adversaries is the need for timely and accurate information to inform our operations. The 2023 DoD Cyber Strategy places renewed emphasis on the role intelligence plays in the planning and execution of cyberspace operations. The Office of the Under Secretary of Defense for Policy is working closely with the Office of the Under Secretary of Defense for Intelligence and Security, and through them, the Defense Intelligence Enterprise, to ensure that the intelligence

requirements of the cyber warfighter are prioritized. The Department will improve business practices and human capital management processes to expand cyber intelligence production and reduce barriers to information sharing consistent with applicable law, policies, and procedures. Consistent with the notification to the Committee by the Secretary, Chairman of the Joint Chiefs of Staff, and Director of National Intelligence, the Dual Hat leadership arrangement, whereby the position of the Director of the National Security Agency and the Commander of USCYBERCOM are held by the same official, is critical to ensuring that our intelligence and military activities are properly integrated.

Conclusion

In conclusion, cyberspace and technology continue to evolve precipitously, requiring the Department and the United States more broadly to anticipate changes and move with the speed and agility necessary to stop those who seek to exploit it. The Department will execute on the path established in the 2023 Defense Cyber Strategy to protect the shared digital environment from those who intend to subvert our values and interests. By pursuing integrated deterrence, which includes our cyber capabilities, the Department will be ready to fight and win the Nation's wars with an ability to respond rapidly across the spectrum of conflict. The Department will make full use of the authorities and capabilities Congress has provided to us as we continue to deter aggression and defend our Nation's security. Thank you for your continued support in this fight and I look forward to answering your questions.



Ashley Manning

Performing the Duties of the Assistant Secretary of
Defense for Cyber Policy

Ashley Manning is currently Performing the Duties of the Assistant Secretary of Defense for Cyber Policy. Previously, she served as both the Acting Deputy Assistant Secretary of Defense and the Principal Director for the Middle East and for Plans and Posture in the Office of the Under Secretary of Defense (OUSD) for Policy. Prior to these positions, she was an exchange officer in the UK Ministry of Defence, where she was the Deputy Head of Strategy and oversaw the development of Defence's contribution to the UK Integrated Review strategy. During her time in OUSD Policy, she has also served as the Director for Global Force Posture and as the Pakistan country director.

Following her selection for the Department of Defense legislative fellows program, she worked in the office of U.S. Representative Michael McCaul and was a visiting fellow at the Washington Institute for Near East Policy. Prior to the fellowship, she served in a number of positions with the U.S. Air Force, managing security cooperation programs with countries in Northeast Asia and South Asia. During her time in government, she has received several awards, to include the Secretary of Defense Meritorious Civilian Service Award, Department of Defense Exceptional Civilian Service Award and the UK Vice Chief of Defence Staff Commendation.

Ms. Manning holds a B.A. in Political Science and an M.A. in Security Studies from The George Washington University. She was also an adjunct professor for several years at the Elliott School of International Affairs, The George Washington University.

POSTURE STATEMENT OF
GENERAL TIMOTHY D. HAUGH
COMMANDER, UNITED STATES CYBER COMMAND
BEFORE THE 118TH CONGRESS
HOUSE COMMITTEE ON ARMED SERVICES
SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION
10 APRIL 2024



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

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

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

(U) WHO WE ARE

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

works closely with Coast Guard Cyber Command within the Department of Homeland Security. Finally, it is important to note our DoD-wide components: our sub-unified command -- the Cyber National Mission Force-Headquarters (CNMF-HQ) -- along with our Joint Task Force Ares, and our Joint Force Headquarters-DoD Information Network (JFHQ-DoDIN).

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

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

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

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

(U) SHIFTING THREATS

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

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

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

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

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

(U) Russia Federation

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

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

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

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

(U) Islamic Republic of Iran

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

(U) USCYBERCOM supports USCENTCOM in its work to deny and deter Iran. In addition, from the outset of the Israel-Hamas war, USCYBERCOM has supported significant efforts to bolster the cyber defenses of Israel and other regional partners. The Command has focused on securing key networks in the region, and provided actionable information, insights, and options to policy makers.

(U) Democratic People's Republic of Korea (DPRK)

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

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

(U) Non-State Actors

(U) Non-state actors remain a threat in cyberspace. Cyber criminals, some operating from Russia and with ties to Russian military and intelligence services, continue to find new victims in the United States and globally. USCYBERCOM and the NSA enable efforts by the Department of the Treasury, the Federal Bureau of Investigation (FBI) and other partners to disrupt ransomware, cryptocurrency theft, and other criminal activities. In addition, violent extremist groups still operate in cyberspace. Though their capabilities have been eroded, the Islamic State in Iraq and Syria (ISIS), al Qaida, and other terrorist groups maintain the intent to target Americans. Our Joint Force Headquarters-Cyber (Marines) works in conjunction with U.S. military and diplomatic efforts, and with allies and partners, to disrupt propaganda and mobilization online as well as to provide critical intelligence.

(U) Technology Change

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

(U) USCYBERCOM IN 2023

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

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

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

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

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

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

(U) USCYBERCOM IN 2024

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

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

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

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

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

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

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

cyberspace and the information environment. We are working to grow uniformed cyber leaders at all levels, up to and including the officers who will eventually succeed me in this post. The staffing and training of our teams improves every year, and the Command's cyber readiness system is now able to ingest data directly from the Defense Readiness and Reporting System without manual input. USCYBERCOM's authorities as Joint Cyberspace Trainer will enable Joint training standards across the entire Department, boosting its ability to defend networks while enabling CMF teams to focus on hunting and contesting foreign adversaries. Additionally, over the past year, we have worked to fill our civilian billets, driving down security and personnel processing times by 25 percent and accelerating hiring actions to fill more than 250 vacancies across the Command. We are using special hiring authorities offered in 10 U.S.C. 4092 to attract top technical talent to join USCYBERCOM. We have made job offers to key experts and look forward to hiring more in 2024. Indeed, we are maximizing use of DoD Cyber Excepted Service authority to streamline civilian hiring and offer competitive employment incentives.

(U) This year will mark the first year in which the Department of the Army is acting as the Combatant Command Support Agent (CCSA) for USCYBERCOM. The Army's military and civilian leaders have been superb in managing this transition and making sure our civilians experience this as a seamless and transparent process. USCYBERCOM is also exploring innovative ways to enhance our operations using the expertise resident in the National Guard and Reserves. We operate side-by-side daily with activated members of the Reserve Component integrated into our teams, and we engage National Guard units on State Active Duty and State Partnership Program engagements.

(U) Strong partnerships with government, industry, academia, and foreign colleagues amplify our effectiveness and create advantages in turn for our partners. Our Components, when working in unison with diplomatic, military, law enforcement, homeland security, and intelligence capabilities, make a powerful combination that can disrupt the plans of malicious cyber actors wherever they hide. In addition, our Regional Cybersecurity and Engagement Strategy in the Indo-Pacific will guide efforts with partners such as Australia, Japan, and South Korea to counter and contest foreign adversaries.

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

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

(U) CONCLUSION

(U) USCYBERCOM creates advantage for the Joint Force, for the Department, for our partners at home and abroad, and most of all for the nation. We work every day against capable

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

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



GENERAL TIMOTHY D. HAUGH

Gen. Timothy D. Haugh is Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service at Fort George G. Meade, Maryland.

Gen. Haugh received his commission in 1991 as a distinguished graduate of the ROTC program at Lehigh University. Gen. Haugh has commanded at the squadron, group, wing, numbered air force and joint levels. He served on staffs at major command, agency and combatant command headquarters.

EDUCATION

- 1991 Bachelor of Arts, Russian Studies, Lehigh University, Bethlehem, Pa.
- 1999 Master of Science, Telecommunications, Southern Methodist University, Dallas, Texas
- 2005 Master of Science, Joint Information Operations, Naval Postgraduate School, Monterey, Calif.
- 2010 Master of Science, National Resource Strategy with a concentration in Information Operations, Industrial College of the Armed Forces, Fort Lesley J. McNair, Washington, D.C.

ASSIGNMENTS

- 1. June 1992–December 1992, Student, Signals Intelligence Officer Course, Goodfellow Air Force Base, Texas
- 2. January 1993–September 1995, Flight Commander, 301st Intelligence Squadron, Misawa Air Base, Japan
- 3. October 1995–July 1998, Commander, Detachment 2, 544th Intelligence Group, Sabana Seca, Puerto Rico
- 4. August 1998–June 2001, Chief, Information Operations Technology Integration, Headquarters Air Intelligence Agency, Kelly AFB, Texas
- 5. June 2001–June 2004, Information Operations Project Officer, Headquarters U.S. Air Force, the Pentagon, Arlington, Va.
- 6. July 2004–September 2005, Student, Naval Postgraduate School, Monterey, Calif.
- 7. September 2005–June 2007, Director of Intelligence, Air Force Special Operations Forces, Hurlburt Field, Fla.
- 8. June 2007–June 2009, Commander, 315th Network Warfare Squadron, Fort George G. Meade, Md.
- 9. July 2009–June 2010, Student, Industrial College of the Armed Forces, Fort Lesley J. McNair, Washington, D.C.
- 10. June 2010–June 2011, Chief, Intelligence, Surveillance, and Reconnaissance Division, 609th Air Operations Center, Al Udeid AB, Qatar
- 11. July 2011–July 2013, Commander, 318th Information Operations Group, Joint Base San Antonio-Lackland, Texas
- 12. July 2013–June 2014, Assistant Vice Commander, Air Force Intelligence, Surveillance, and Reconnaissance Agency, JB San Antonio-Lackland, Texas
- 13. June 2014–May 2016, Commander, 480th ISR Wing, JB Langley-Eustis, Va.
- 14. June 2016–June 2017, Deputy Commander, Joint Task Force-Ares, U.S. Cyber Command, Fort George G. Meade, Md.
- 15. June 2017–June 2018, Director of Intelligence, U.S. Cyber Command, Fort George G. Meade, Md.
- 16. June 2018–August 2019, Commander, Cyber National Mission Force, Fort George G. Meade, Md.
- 17. August 2019–October 2019, Commander, Twenty-Fifth Air Force, JB San Antonio-Lackland, Texas
- 18. October 2019–August 2022, Commander, Sixteenth Air Force; Commander, Air Forces Cyber, and Commander, Joint Force Headquarters-Cyber, JB San Antonio-Lackland, Texas
- 19. August 2022–February 2024, Deputy Commander, U.S. Cyber Command, Fort George G. Meade, Md.
- 20. February 2024–present, Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service, Fort George G. Meade, Md.

SUMMARY OF JOINT ASSIGNMENTS

- 1. June 2001–June 2004, Information Operations Project Officer, Headquarters U.S. Air Force, the Pentagon, Arlington, Va., as a



EFFECTIVE DATES OF PROMOTION

Second Lieutenant December 09, 1991	
First Lieutenant December 09, 1993	
Captain December 09, 1995	
Major September 01, 2002	
Lieutenant Colonel March 01, 2006	
Colonel August 01, 2011	
Brigadier General November 02, 2016	
Major General August 30, 2019	
Lieutenant General October 11, 2019	
General February 02, 2024	

4/8/24, 9:14 AM

TIMOTHY D. HAUGH

major

2. June 2007–June 2009, Commander, 315th Network Warfare Squadron, Fort George G. Meade, Md., as a lieutenant colonel
3. June 2010–June 2011, Chief, Intelligence, Surveillance and Reconnaissance Division, 609th Air Operations Center, Al Udeid Air Base, Qatar, U.S. Central Command, as a colonel
4. June 2017–June 2018, Director of Intelligence, U.S. Cyber Command, Fort George G. Meade, Md., as a brigadier general
5. June 2018–August 2019, Commander, Cyber National Mission Force, Fort George G. Meade, Md., as a brigadier general
6. August 2022–February 2024, Deputy Commander, U.S. Cyber Command, Fort George G. Meade, Md., as a lieutenant general
7. February 2024–present, Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service, Fort George G. Meade, Md., as a general

MAJOR AWARDS AND DECORATIONS

- Distinguished Service Medal
- Defense Superior Service Medal
- Legion of Merit with two oak leaf clusters
- Bronze Star Medal
- Defense Meritorious Service Medal
- Meritorious Service Medal with four oak leaf clusters
- Joint Service Commendation Medal with three oak leaf clusters
- Air Force Commendation Medal
- Air Force Achievement Medal

(Current as of February 2024)



DOCUMENTS SUBMITTED FOR THE RECORD

APRIL 10, 2024

March 25, 2024 | Monograph

United States Cyber Force

A Defense Imperative

Dr. Erica Lonergan **RADM (Ret.) Mark Montgomery**
Columbia University CCTI Senior Director and Senior Fellow

Executive Summary

In the U.S. military, an officer who had never fired a rifle would never command an infantry unit. Yet officers with no experience behind a keyboard are commanding cyber warfare units. This mismatch stems from the U.S. military's failure to recruit, train, promote, and retain talented cyber warriors. The Army, Navy, Air Force, and Marines each run their own recruitment, training, and promotion systems instead of having a single pipeline for talent. The result is a shortage of qualified personnel at U.S. Cyber Command (CYBERCOM), which has responsibility for both the offensive and defensive aspects of military cyber operations.

For the last decade, Congress, on a bipartisan basis, has made clear its sharp concern about cyber personnel issues. In 2022, it required the secretary of defense to deliver a report that addresses "how to correct chronic shortages of proficient personnel in key work roles" at CYBERCOM. The report is due on June 1.¹

Often, however, military leaders have addressed personnel shortages by massaging statistics rather than fixing the underlying problem. In 2018, CYBERCOM appeared to reach a major milestone when it certified that all 133 of its Cyber Mission Force (CMF) teams had enough properly trained and equipped personnel to execute their missions. Yet multiple officers revealed these certifications to be hollow; CYBERCOM merely shifted a limited number of effective personnel from team to team to make them appear complete at the time of certification.

To deepen the understanding of the cyber personnel system and its flaws, this study draws on more than 75 interviews with U.S. military officers, both active-duty and retired, with significant leadership and command experience in the cyber domain.² The study identifies these officers by rank and service but withholds their names for reasons of privacy.

This research paints an alarming picture. The inefficient division of labor between the Army, Navy, Air Force, and Marine Corps prevents the generation of a cyber force ready to carry out its mission. Recruitment suffers because cyber operations are not a top priority for any of the services, and incentives for new recruits vary wildly. The services do not coordinate to ensure that trainees acquire a consistent set of skills or that their skills correspond to the roles they will ultimately fulfill at CYBERCOM. Promotion systems often hold back skilled cyber personnel because the systems were designed to evaluate servicemembers who operate on land, at sea, or in the air, not in cyberspace. Retention rates for qualified personnel are low because of inconsistent policies, institutional cultures that do not value cyber expertise, and insufficient opportunities for advanced training.

Resolving these issues requires the creation of a new independent armed service — a U.S. Cyber Force — alongside the Army, Navy, Air Force, Marine Corps, and Space Force. There is ample precedent for this approach; battlefield evolutions led to the establishment of the Air Force in 1947 and the Space Force in 2019. An independent cyber service would naturally prioritize the creation of a uniform approach to recruitment, training, promotion, and retention of qualified personnel whose skills correspond to CYBERCOM's needs. In addition to a single, dedicated cyber training and development schoolhouse, an independent service could establish a cyber war college for advanced research and training, akin to the Army War College and its peers. Without the responsibility for procuring planes, tanks, or ships, a Cyber Force could also prioritize the rapid acquisition of new cyber warfare systems.

This Cyber Force need not be large. An examination of existing cyber billets suggests it would initially comprise about 10,000 personnel but might grow over time. As the Space Force has shown, a smaller service can be more selective and agile in recruiting skilled personnel.

Some military experts have proposed alternative approaches to addressing the U.S. military's cyber personnel shortage, but each has major shortcomings. For example, some argue that CYBERCOM should become more like the U.S. Special Operations Command, to which each service provides elite personnel uniquely trained for the land, sea, and air domains. But that model makes little sense for cyberspace since there are no cyber functions specific to the other warfighting domains. Others argue CYBERCOM should assume responsibility for manning, training, and equipping cyber forces in addition to employing them on the virtual battlefield. But this approach would break with 40 years of precedent and would overwhelm CYBERCOM's leadership, which is already dual-hatted with the National Security Agency, an arrangement that serves U.S. national security well.

America's cyber force generation system is clearly broken. Fixing it demands nothing less than the establishment of an independent cyber service.

Illustrated prospective seal for U.S. Cyber Force (Design by Daniel Ackerman/FDD)

History and Current Organization of the U.S. Military in Cyberspace

For nearly 40 years, the U.S. military has separated the responsibility for force generation—the imperative to “man, train, and equip” personnel for their specific domains—from the responsibility of force employment—the use of troops in combat. The independent services—the Army, Navy, Air Force, Marine Corps, and Space Force—generate forces, while the unified combatant commands employ forces and can request manpower from each of the services.

For every domain but cyberspace, the United States has designated a single service as the one ultimately responsible for force generation for its respective domain. For example, while the Army, Navy, and Marine Corps operate significant aircraft fleets, it is primarily the Air Force's responsibility to man, train, and equip U.S. troops for air combat.

Since the establishment of CYBERCOM in 2010 and its subsequent elevation to a unified combatant command in 2018, the military has had a designated organization for force employment in and through cyberspace. But the United States still has no single entity responsible for cyber force generation.

The Creation of CYBERCOM

The pivotal role of advanced technology in the 1991 Gulf War led the Department of Defense (DoD) to recognize the importance of what were then known as “computer network operations.”³ The U.S. military began developing cyber doctrine in earnest in 2003 after the discovery of a multi-year Russian cyber espionage operation revealed the “first large-scale cyberespionage attack by a well-funded and well-organized state actor.”⁴ The next year, the Joint Chiefs of Staff defined cyberspace as a warfighting domain,⁵ and DoD released its first National Military Strategy for Cyberspace Operations in 2006.⁶ (A more detailed account can be found in Appendix C.)

After discovering additional foreign cyber espionage campaigns targeting the department, DoD in 2010 combined existing cyber elements to establish CYBERCOM under U.S. Strategic Command. CYBERCOM is led by a commander dual hatted as director of the National Security Agency (NSA), the intelligence community component responsible for signals intelligence and cybersecurity services. CYBERCOM became responsible for defending DoD information systems, supporting joint force commanders in cyberspace, and advancing national interests in and through cyberspace.

The services also developed their own components responsible for information and cyber operations in support of operations in their respective warfighting domains. These components include what are now the 16th Air Force, Army Cyber Command, Fleet Cyber Command, and Marine Corps Forces Cyberspace Command.

In 2018, the president elevated CYBERCOM to a unified combatant command. This move retained the dual-hatted structure and gave CYBERCOM a direct line of communication to the secretary of defense plus greater authority to request budgetary resources.⁷

Despite standing up CYBERCOM, the military has not established a cyber-specific training academy. In other areas, institutions such as the U.S. Army War College, U.S. Naval War College, Air War College, U.S. Marine Corps University, and National Defense University provide specialized training for senior enlisted personnel and officers, preparing them for leadership positions and assignments in the joint force. This is known as force development.⁸

The 2019 National Security Commission on Artificial Intelligence argued for the creation of a Digital Service Academy to address talent deficits in the defense and intelligence communities.⁹ DoD's failure to implement this recommendation after three years and multiple congressional initiatives¹⁰ suggests such an academy will not succeed absent an independent service that can deliver the expertise and resources to equip a cyber-specific service academy.

Current Organization of the U.S. Military in Cyberspace

The U.S. military's Cyberspace Operations Forces (COF)¹¹ encompass elements that conduct reconnaissance, operational preparation of the environment, and network-enabled operations, along with subordinate logistics and administrative elements.¹² In addition, the COF includes DoD network operations centers and cybersecurity service providers that conduct traditional network defense and information technology (IT) support functions. This latter group makes up the bulk of COF personnel.¹³ Separately, some U.S. military cyber personnel, serving outside the COF, conduct traditional business functions, protect service-specific systems, and support other functional or geographic commands (see Figure 1 below).

Figure 1: Cyberspace Operations Forces

Within the COF, the Cyber Mission Force directs, coordinates, and executes cyber operations. It comprises less than 3 percent of the COF, or approximately 6,200 military and civilian personnel.¹⁴ The CMF currently includes 133 teams. But in 2022, DoD announced the CMF would expand to 147 teams, including:¹⁵

- Thirteen Cyber National Mission Force (CNMF) teams responsible for "defend[ing] the nation by seeing adversary activity, blocking attacks, and maneuvering in cyberspace to defeat them." These operations are largely conducted as independent campaigns, not in support of combatant command missions.
- Twenty-seven Cyber Combat Mission Teams, which "conduct military cyber operations in support of combatant commands."
- Sixty-eight Cyber Protection Teams responsible for "defend[ing] the DOD information networks, protect[ing] priority missions, and prepar[ing] cyber forces for combat."
- Twenty-five Cyber Support Teams, which provide analytic and planning support to CNMF and the Cyber Combat Mission Teams.¹⁶
- Fourteen new teams responsible for supporting combatant commanders in space operations and countering cyber influence.

In 2018, CYBERCOM attested that the original 133 CMF teams achieved full operational capacity (FOC). In other words, each team ostensibly had the ability to fully employ its cyber weapons with adequately trained, equipped, and supported servicemembers.¹⁷ Of those 133 CMF teams, 41 came from the Army, 40 from the Navy, 39 from the Air Force, and 13 from the Marine Corps.¹⁸

In 2022, the CNMF became a sub-unified combatant command, endowing it with additional authorities and responsibilities. Its commander explained that this status will enable CNMF to build “a force that can move faster than our adversaries, because we have the right set of equipment, the right authorities, and the right procedures that move with agility and speed.”¹⁹

The 14 additional CMF teams are supposed to be stood up between fiscal years 2022 and 2026. Five of the new teams are slated to come from the Army, with the Air Force and Navy providing five and four, respectively.²⁰ By mid-2023, however, it became clear that CYBERCOM would need to delay its plans. In particular, the Navy will not be able to deliver new teams for at least a few years because it needs to focus on improving the readiness of its existing cyber personnel.²¹

Moreover, even the existing teams have not actually reached FOC despite what CYBERCOM claims.

Evolution of CYBERCOM's Authorities

While CYBERCOM has had the authority to conduct operations short of armed conflict outside of DoD-controlled networks since its creation,²² the Fiscal Year (FY) 2019 National Defense Authorization Act (NDAA) legislated the most important change in CYBERCOM's authorities, defining cyber operations as a “traditional military activity,” and authorized DoD (and, by extension, CYBERCOM) to act in “foreign cyberspace to disrupt, defeat, and deter” cyberattacks against the U.S. government and the American people.²³ This change allowed for more extensive planning and execution of cyber operations. The new authority also largely aligned with National Security Presidential Memorandum-13 (NSPM-13), a Trump administration initiative to streamline the process for authorizing military cyber operations.²⁴ The Biden administration reportedly modified NSPM-13 but has largely kept it in place.²⁵

CYBERCOM has also gained new acquisition authority and statutory responsibility for managing personnel. Previously, the services served as the executive agents for procurement for CYBERCOM, although CYBERCOM also possessed limited acquisition authority to execute contracts, with a \$75 million annual cap. Then, in the FY 2022 NDAA, Congress took the unusual step of providing CYBERCOM with Enhanced Budgetary Control (EBC) to directly manage resources for equipping the CMF.²⁶ These EBC authorities, which will take full effect this year, reflect congressional frustration with failures in the existing, services-led acquisition efforts on CYBERCOM's behalf. As then CYBERCOM commander General Paul Nakasone explained to Congress in March 2023, the hope is that EBC will better harmonize CYBERCOM's responsibilities and operations by providing it with control over funding for major acquisition programs.²⁷

Nevertheless, the lion's share of cyber funding in the FY 2024 budget remains with the services. CYBERCOM's budget request is approximately \$2.9 billion, while DoD's total Cyberspace Activities Budget request for the services is \$13.5 billion.²⁸ Moreover, CYBERCOM will still rely on the services to spend much of the money that Congress appropriates.²⁹

The promise of EBC was that it would bring CYBERCOM closer to the U.S. Special Operations Command (SOCOM) model, in which the force employer helps guide procurement. However, the services still retain the vast majority of cyber-specific funding, continuing CYBERCOM's dependency on the services. The persistent structural problems render CYBERCOM unable to provide for itself. It continues to rely on the military services and, in some circumstances, the NSA for personnel, funding, foundational intelligence support, procurement and acquisition activities for cyber-specific capabilities, research and development for tools, and infrastructure supporting cyber operations.

Congressional Concerns About CYBERCOM's Insufficient Maturity

Over the past five years, CYBERCOM has achieved important operational successes. It has conducted “hunt forward” operations at the invitation of allied and partner nations to help uncover and defeat cyber threats in their networks.³⁰ It has also defended U.S. elections,³¹ responded to Iranian hackers in Albania,³² and helped Ukraine shore up its cyber systems following Russia's 2022 invasion.³³ However, these successes came despite, not as a result of, the U.S. military's current organization for cyberspace operations.

Congress has repeatedly raised concerns about these issues. At a March 2023 hearing, Rep. Mike Gallagher (R-WI) noted: “Since 2013, Congress has tried to address force design and readiness through 24 different pieces of legislation. Twenty-four. And over that same period, we have tried to address the civilian and military cyber workforce dilemma 45 times; CYBERCOM acquisition matters, 12 times; and defense industrial base cybersecurity, 42 times.”³⁴

Nearly every year for the past decade, Congress has requested information or reports about military cyber readiness — a clear indication DoD has been unable to satisfy congressional concerns. In 2016, Congress mandated that CYBERCOM launch an expedited two-year force-generation effort because the CMF had not achieved sustainable readiness.³⁵ The next year, Congress requested briefings on cyber readiness shortfalls.³⁶ In the FY 2020 NDAA, Congress required the secretary of defense to analyze the benefits and drawbacks of “establishing a cyber force as a separate uniformed service.”³⁷ Two years later, Congress again called for an assessment of U.S. cyber posture.³⁸

Subcommittee Chairman Rep. Mike Gallagher (R-WI) (2nd L) listens during a hearing before the Cyber, Information Technology, and Innovation Subcommittee of the House Armed Services Committee on Capitol Hill on March 30, 2023 in Washington, DC. (Photo by Alex Wong/Getty Images)

The FY 2023 NDAA directed the secretary of defense to study the services' responsibilities for cyber force generation in light of "chronic shortages of proficient personnel in key work roles."³⁹ Among other issues, the study is supposed to explore whether a single military service should be responsible for force generation.

CYBERCOM implicitly acknowledged its force generation challenges in its May 2023 Strategic Priorities, vowing to improve readiness, recruitment, and retention.⁴⁰ DoD, meanwhile, is developing a so-called "Cyber Command 2.0" initiative to address how the military generates and trains cyber forces.⁴¹ In December 2023, General Nakasone observed that the current state of U.S. military cyber organization is unsustainable. "I think all options are on the table, except the status quo," he said.⁴²

In Their Own Words: Gaps and Challenges in the Current Model

While force employment is the responsibility of CYBERCOM, responsibility for force generation is spread across the five military services. This system is failing to meet the unique demands of cyber-related training and acquisition. As one general officer lamented, "Our current strategy of relying on the existing Services to build the cyber expertise and capabilities required is inefficient, ineffective, and unlikely to succeed despite years of investment and the best efforts of our servicemembers." Washington's "only viable path forward," the officer said, "is to establish a new Service focused on organizing, training, and equipping forces required to fight – and win – in cyberspace."⁴³

Manning and training for cyberspace operations are not equivalent to furnishing infantry or logistics personnel. All specialties have distinct training and skill requirements, but the cyber domain requires a uniquely high level of technical training. As a result, individual cyber personnel can have outsized operational effects. As one lieutenant colonel in the Air Force noted, "10% of the [cyber] workforce provides 90% of the value."

Additionally, acquisition processes for equipment and capabilities must move far more quickly than those for the other warfighting domains. Acquisition of software or exploits, for example, must occur rapidly to ensure they are not rendered obsolete.⁴⁴ Moreover, many of the most cutting-edge capabilities reside within the private sector, including in industries not traditionally part of the defense-industrial base. Finally, there is a potentially greater role for non-uniformed civilian personnel in cyberspace capability development and employment.

The current system compounds these force-generation challenges. Each of the services has developed its own solutions, leading to both inconsistencies and shortcomings. As outlined below, these issues span talent recruitment and retention; occupational designations and training; promotions; critical support functions; administrative control; and capability acquisition.⁴⁵

At root, the current readiness issue stems from the fact that none of the existing services prioritizes cyberspace. As a retired Navy captain observed, this fundamental mismatch "has yielded varying levels of fragmented support to cyber operations, [a] lack of continuity of cyber personnel, unclear career paths, insufficient experience, wide use of non-cyber personnel in cyber leadership positions, and cyber operations being treated always as a supporting entity across all services."

The extensive interviews that inform this study provide the most direct and compelling evidence to date of the deficiencies in the U.S. military's current cyber force generation model and readiness. They also help explain why the establishment of a Cyber Force is the best and only solution to these challenges. (See Appendix A for excerpts from the interviews and a demographic breakdown of the interviewees.)

Recruitment and Retention Shortfalls

The U.S. military is failing to recruit and retain enough talented cyber personnel. The "lack of talented personnel to fill positions on the Cyber Mission Force has been and continues to be a severely limiting factor for the overall force," one Army colonel explained. A 2022 Government Accountability Office (GAO) report similarly concluded that all the services "continue to experience challenges retaining qualified cyber personnel." Even the Army, which has fared better in the recruitment of skilled cyber personnel, has struggled to retain its cyber workforce.⁴⁶

The current recruitment and retention shortfall stems from multiple problems, some of them inherent to the current system. First, the services are not using the tools at their disposal to bolster compensation for high-caliber personnel, nor are the services compensating them equitably. In addition, the services have inconsistent and poorly designed requirements governing how long their warfighters must serve. Worse, retention suffers from problems with service culture, leadership, and quality of life. The services' promotion systems and CYBERCOM's lack of administrative support also undermine retention, as discussed later in the report.

A Cyber Force would be far better equipped to recruit and retain cyber personnel, as the success of the Space Force has shown. Despite competing with private sector firms that offer more attractive salaries, the Space Force has not faced problems recruiting high-level talent.⁴⁷ Because it is relatively small, the Space Force can selectively recruit highly skilled individuals rather than pursuing bulk accessions to fill the ranks like the larger services.⁴⁸

SERVICES FAIL TO USE TOOLS AT THEIR DISPOSAL

To be fair to the services, the U.S. military is not the only one struggling to recruit cyber talent. There is a national shortage of cyber personnel, and the federal government struggles to compete with the private sector, which offers much better pay.⁴⁹

Unlike the military, civilian government agencies use creative promotion schemes to ensure their cyber workforce is well-compensated, even if salaries do not match the private sector. The military also has some tools it can use to improve compensation, but the services are not using them effectively. For example, the 2022 GAO study found that the Army was not offering enlistment bonuses to cyber personnel.⁵⁰

As one Army captain explained, CYBERCOM itself "is not able or empowered to use these options." Meanwhile, "the service components responsible for manning CYBERCOM refrain from pursuing these choices aggressively because cyber is only one mission and not their primary charge." A Cyber Force, by contrast, would naturally put cyber first.⁵¹

INCONSISTENT COMPENSATION

In addition to being inadequate, U.S. military compensation for cyber personnel is inconsistent across the services, damaging morale and esprit de corps.

Once the services recruit personnel, each service separately determines which ranks serve in which jobs. The Marines might assign a staff sergeant (E-6) to the same job the Air Force assigns a first sergeant (E-8). With different pay scales and incentives for these different ranks, the result is wide pay discrepancies between individuals performing identical work. Even when the servicemembers have similar levels of experience, compensation varies significantly. For example, the monthly salaries of two Interactive On-Net Operators (IONs) from different services, each with four to five years of experience, serving in the same location and performing largely the same job, may differ by more than \$700.⁵² This discrepancy does not even take into account differences in housing allowances or pay incentives.

GAO studies have found that enlistment bonuses also vary dramatically across the services. Whereas GAO found in 2022 that the Army was not offering enlistment bonuses, the Marine Corps was offering \$2,000 for cyber career fields, and the Navy was offering \$5,000 with an additional \$30,000 bonus after training completion.⁵³

The services also use bonuses and incentives inconsistently and without regard for who is a worthy recipient. According to the 2022 GAO study, the services base retention bonuses for cyber personnel on their broader military career, not their unique skill sets.⁵⁴ These findings matched conclusions from a 2017 GAO study.⁵⁵ The persistence of these issues five years after the initial GAO study underscores that the services cannot fix these problems themselves.

INCONSISTENT AND POORLY DESIGNED LENGTH-OF-SERVICE REQUIREMENTS

Low cyber retention rates stem in part from inconsistent and poorly designed length-of-service requirements. Because each service has its own retention policies, they have distinct requirements for how long their servicemembers, including cyber personnel, must remain on active duty. What is more, these requirements do not adequately account for the "lengthy and expensive advanced cyber training" provided to cyber personnel, according to the GAO.⁵⁶

For example, the Army usually requires officers to serve three times the length of their training. However, many advanced cyber training courses are not included in this Army regulation. As a result, personnel could attend an expensive year-long cyber training course and leave the military soon afterward.⁵⁷ Until legislative intervention in 2023, the Marine Corps could not assign additional service obligations for lengthy and expensive cyber training.⁵⁸

CULTURE

Many officers have described how service culture denigrates cyber talent, damaging the morale of cyber personnel and eroding retention.⁵⁹ Retention rates of cyber personnel are abysmal, "one retired Navy captain remarked. "The biggest reason the services hemorrhage talent is that cyber personnel do not feel valued by their service's culture." Similarly, a retired Army colonel shared, "I've seen senior warfighting leaders dismissively call cyber research 'book reports,' cyber operators 'nerds,' and cyber capability development 'science projects.'" Only the creation of a new service dedicated to cyberspace can address these kinds of entrenched cultural challenges.

Inconsistent Career Field Designations, Skill Sets, and Training

Across the services, cyber-related career field assessments, assignments, designations, and skill sets⁶⁰ are ill-defined and disjointed. This fragmented approach undermines training and personnel management.

INCONSISTENT AND INADEQUATE TRAINING

Currently, servicemembers arrive at CYBERCOM with skill sets that are not only inconsistent but also insufficient to fulfill their basic work roles. This problem stems from each of the services not only using different names for their cyber operators but also training them differently—without CYBERCOM's needs in mind.

For example, when an Air Force cyber operations officer, a Navy cyber warfare engineer, and a Marine Corps cyber operations officer complete their initial entry training, they lack a common skill set (such as knowledge of specific operating systems or exploits). And none are qualified to serve in any of CYBERCOM's basic work roles upon arrival.

In fact, it was not until February 2023 that the Navy began using a separate designation for its cyber warfare officers, in alignment with how the other services treat their cyber operations experts.⁶¹ While the Army and Air Force generally enable personnel to devote their careers to cyber roles, the Navy had been grouping cyber officers with intelligence and information warfare officers, hampering their ability to develop expertise.

The services train cyber personnel at service-specific training centers. Army centers include the Army Cyber School's Virtual Training Area, the U.S. Army Cyber Center of Excellence, and Fort Eisenhower Signal Training Site. Air Force personnel train at the Air Force Cybersecurity University and the Cyberspace Technical Center of Excellence. The Navy has the Naval Information Warfare Training Center and the Naval Postgraduate School Center Cybersecurity and Cyber Operations. Finally, there is the Marine Corps Air/Ground Combat Center in California.

These centers do not have a common training system or set of standards. As one Navy captain noted, "Each service has developed their own training model and paths, which do have some overlap but for the most part are not synchronized." They each have "different service-desired outcomes and minimal joint perspective when outside of CNMF roles," the captain explained. "Without one overarching cyber service and related vision and clearly defined mission, cyber training will continue to produce an unbalanced and ineffective joint workforce where services will continue to prioritize efforts and service-specific career paths."

A Navy lieutenant commander agreed. "Each of these services are [sic] training and employing cyber personnel to do the exact same jobs, such as exploitation analyst, tool developer, and cyber planner," the officer observed. "Despite these identical needs, there is virtually no standardization whatsoever across the entirety of the military workforce. Each separate service maintains its own training programs, its own performance evaluation processes, its own employment metrics." In short, "the totality of the force is wholly uncoordinated. From a mission perspective, I have witnessed firsthand how this situation creates impossible problems with regard to technical expertise and training."

Many other officers discussed the lack of specialization in operating systems, intelligence, exploits, and other techniques associated with cyber-related personnel across the services. Instead of offering specialized training, the services provide general coursework, teach capabilities at a high level of generality, and require operators to learn a broad range of system architectures rather than honing

their skills on a specific system. This is like requiring Air Force pilots to learn a bit about all types of aircraft in the fleet rather than specializing in the particular craft they will pilot.

Figure 2 contrasts CYBERCOM-defined work roles with service-specific cyber career field designations and titles for both officers and enlisted personnel.⁶² There is little overlap between the two. Furthermore, the service-based training with each military occupational specialty (MOS) does not slot into any particular CYBERCOM work role.

Figure 2: Service-Specific Cyber Career Field Designations and CYBERCOM Work Roles

Compared to the other warfighting domains, the U.S. military spends relatively little time and money on training for cyber officers. The initial cost of training an Air Force fighter pilot ranges from \$5.6 to \$10.9 million, and the annual cost of training for a Naval aviator is \$2.2 million, according to a RAND report.⁶³ By contrast, the GAO found that the training and subsequent certification to become an interactive on-net operator costs between \$220,000 and \$500,000.⁶⁴

The GAO also found that courses are "not listed in regulation or in Army or joint training systems of record." There are long breaks between courses, and the length of the courses themselves fluctuates. In addition, there are often significant delays between when candidates are nominated for training and when they attend.⁶⁵

Across the services, there is also a lack of continual training for the officer corps. An April 2023 paper published by the National Defense University concluded that the cyber domain requires continual training with some technical training delivered every 18 to 24 months.⁶⁶ Although servicemembers often have the opportunity to attend graduate school, such courses are also not well suited to technical training for a dynamic, rapidly changing field. Such courses are also different from the more specialized cyber upskilling needed to create effective leaders.

INABILITY TO MANAGE CYBER PERSONNEL

Because the services do not designate personnel for particular CYBERCOM work roles, "military service officials cannot determine if specific work roles are experiencing staffing gaps," the GAO concluded. Put simply, the services do not know if they have "the right personnel to carry out key missions."⁶⁷

Likewise, there is no system or method to track individuals with cyber skills as they transition to and from the services and CYBERCOM. This means a servicemember may enter with initial training for a cyber-related career field but could be moved to a non-cyber career track during one of these transitions. Such reassignments stem from the reality that the services understandably prioritize their unique needs and missions, which may not allow for individual personnel to stay on a cyber-specific track for the duration of their career.⁶⁸

Promotion Processes Do Not Reward Technical Competence

The services determine promotions for their cyber personnel, but they use systems designed for the non-cyber world. These systems reward command experience — usually in non-cyber fields — over technical competence. As a result, the services are replete with commissioned and non-commissioned officers who may be good leaders but lack the cyber-specific skills and experience necessary to excel.

Standard service processes require an individual to have held certain positions to be promoted. These roles are often entirely unrelated to CYBERCOM priorities. In the Army, for example, a lieutenant must serve as a platoon leader before being promoted. But many technically proficient cyber operators never hold the positions deemed necessary for advancement. Consequently, they are passed over for promotion, while those without cyber expertise are placed in command.

Compounding this issue, the personnel in charge of the promotion process within each service typically lack the requisite cyber knowledge to make effective promotion decisions. A U.S. Army colonel noted that the individuals on service promotion boards struggle to differentiate between "officers with advanced, skilled degrees in computer science from esteemed institutions" and "those who received online degrees in information management. ... This is akin to equating a brain surgeon with a field medic."

It does not have to work this way. The Space Force provides an illustration. As a first lieutenant in the Air Force explained, the "Space Force gives the best-qualified commanders the best-qualified experts (long-time members who have reached the major, lieutenant colonel, or warrant officer levels), and those experts retain the ability to work a technical role while still benefiting from career progression." By contrast, the current promotion system for cyber "robs all highly technical career fields of their most qualified experts, as our antiquated career progression system demands they go on to command something rather than do their best work at the keyboard."

The current promotion system creates real risks to U.S. security. In a June 2023 military journal article, Navy Reserve Lieutenant Commander Eric Seligman notes that officers without cyber warfare experience struggle to assess the risks stemming from cyber operations. They face decision paralysis, improperly staff subordinate positions, and often fail to employ technical solutions necessary to achieve operational and tactical objectives. They also have difficulty translating doctrine into action, distinguishing good from bad operational and tactical advice, and predicting enemy maneuvers.⁶⁹

As Seligman argues, a doctrinal and policy-focused understanding of cyber warfare is no replacement for hands-on experience. It would be like an officer who has "been trained on the concept of the rifle and its potential effects on the enemy" but never actually fired one.⁷⁰ Marine Corps officers stand by the tenet, "Every Marine a rifleman." No Navy SEAL would follow an officer into battle if that officer did not go through BUD/S training. However, cyber operators and junior officers today follow the orders of a mostly inexperienced senior officer cadre. A Marine Corps captain concurred, "Leading in the cyberspace domain demands technical competency that cannot be taught in a 12-month schoolhouse alone." He added, "Under no circumstances would a cyber officer be asked to lead a squadron of aircraft, and yet the opposite is often true."

Indeed, interviewees for this project cite numerous examples of senior officers who have little to no experience in the cyber domain—even though the services have had 13 years since the creation of CYBERCOM to develop qualified senior leaders. Of the U.S. military's more than 45 general and flag officers involved in cyber as of summer 2023, fewer than five had any technical experience in the cyber domain.⁷¹

CYBERCOM today has promotable talent, but the military is not properly utilizing it. A Marine Corps captain stated that he "personally had career setbacks because (he) pursued a master's degree in computer science instead of a military war-college certificate."

The current promotion system creates a vicious cycle. Potential cyber leaders cannot look to their superiors for mentorship or wisdom gained from experience within the domain. Facing disincentives to the further development of their skills, talented cyber officers choose other paths or exit the military altogether, depriving the next generation of cyber-experienced leadership.

Lack of Administrative, Intelligence, and Mental Health Support

CYBERCOM lacks many of the dedicated support functions that other unified combatant commands enjoy, including foundational intelligence support for operations, administrative support, and medical support, especially for mental health.

ADMINISTRATIVE SUPPORT

Too often, CYBERCOM's few qualified cyber operators are pulled away from operational responsibilities to handle administrative functions because the services provide CYBERCOM with inadequate administrative support. "Very few capable analysts can dedicate a significant amount of time to the operational mission," a U.S. Air Force major commented. "Less than 10 percent of team members have been on the team for over a year," placing a significant burden on the few experienced analysts to both execute operations and train new personnel. The CNMF's elevation to a sub-unified command in December 2022 partly resolved this issue, but the CNMF is only one-third of the CMF. The other teams continue to lack administrative support.

The administrative burden foisted onto cyber operators undermines talent retention. A 2019 internal survey of the U.S. Army Cyber Command workforce found that "a factor in their decision to leave after their contracts or service obligations expired was their inability to focus on the mission or tradecraft (i.e., time spent on keyboard) due to the constant distractions from administrative requirements."⁷²

INTELLIGENCE SUPPORT

Cyber reconnaissance and targeting support are essential to the effectiveness of offensive cyber operations but CYBERCOM currently receives inadequate intelligence support.⁷³

4/23/24, 12:48 PM

United States Cyber Force

Like all combatant commands, CYBERCOM does have a Joint Intelligence Operations Center, which provides operational intelligence for force employment. Cyber operations, however, lack a dedicated all-source cyberspace intelligence center to collect foundational, ongoing intelligence about adversary cyber capabilities and order of battle. The U.S. military does have such centers for other warfighting domains, such as the Army's National Ground Intelligence Center or the Navy's Office of Naval Intelligence. These centers address standing intelligence requirements about adversary capabilities and strategies. Last year, the outgoing commander of CYBERCOM's Joint Intelligence Operations Center called the absence of a comparable center for cyber intelligence a "gaping hole."⁷⁴

In 2023, CYBERCOM announced it would establish a foundational cyber center in partnership with the Defense Intelligence Agency (DIA) and NSA. In effect, CYBERCOM attempted to build a service-like capability to remediate the gaps stemming from the absence of an independent cyber service. The final version of the FY 2024 NDAA, however, did not include the proposed provision to establish such a center.⁷⁵

If such a center were established, it would likely suffer staffing shortages unless the United States also creates a Cyber Force. The resourcing and staffing for existing intelligence entities usually falls to the parent service. While the DIA (or others) could be charged with managing the center, it would fall to the existing services to provide trained and qualified personnel, who would likely face the same training and skill development issues described earlier.

MEDICAL SUPPORT

Cyber operators work in intense environments but are not afforded the same downtime as their counterparts in other fields.⁷⁶ Mental health initiatives exist across the DoD, including for Special Operations Forces, pilots, and operators involved with unmanned aerial flight operations.⁷⁷ However, there are no programs for the distinct challenges faced by cyber personnel.

Without an understanding of the work roles and tasks of cyber operators, the services (and specific commanders) may not appreciate the need for mental health services. One officer shared his troubling experience: "I think many folks in military cyber have been struggling with inexperienced leadership. But in [my service], those put in charge of cyber units can be downright hostile to technical cyber officers. For example, how about getting retaliated against by your [commanding officer] and your chain of command simply for going to mental health [treatment]? That thing they said in the yearly [general military training] about how going to mental health won't affect your clearance ... it happened to me."

Service Control and Service-Related Requirements Degrade Full Operational Capability

"Years of investment and training are lost when servicemembers are moved away from the cyber mission," a general officer lamented. But because the services retain administrative control over cyber personnel assigned to CYBERCOM, the services can pull them out for service-related requirements unrelated to their cyber roles. This is one important reason why CYBERCOM was unable to get all 133 CMF teams up to FOC status and why it is so difficult for teams to maintain that status.

A lieutenant colonel in the U.S. Army Reserves, speaking from personal experience at the CNMF, observed a "general tension" between the administrative control and operational control commands. "[W]e are forced to pull servicemembers away from operational tasks to instead conduct service-related activities ... This is a systemic problem that, in mine and others' opinions, hurts retention, as it undermines morale," the officer said. Administrative control commanders "often create requirements at the expense of the mission. There are well documented times when units have closed down joint mission areas en masse to conduct unit events."

An Air Force major shared a similar experience: "In one instance, a group commander required a 12-week 'life skills' course that taught new airmen how to cook, how to date, and how to be emotionally healthy. Meanwhile, the mission was manned at less than 60 percent." The major said, "Another commander cited an 'unwritten rule' stating that he only owed the [NSA] 80 percent of his airmen's time and the other 20 percent belongs to the USAF."

In addition to impinging on cyber operators' time, the services can also rotate them to different, non-cyber assignments. As one Army colonel explained, "Upskilling talent is hard, takes years, and as soon as someone reaches a threshold, the service rotates that person out of the team and back to a service assignment ... The demands within the services are continuing to pull talent away from the CMF."

THE SERVICES' FOC SHELL GAME

By 2018, all the existing CMF teams had officially reached FOC, meaning they were supposed to have sufficiently trained and equipped personnel to execute their missions.⁷⁸ Yet fewer CMF teams are actually at FOC than official metrics indicate.

First of all, the services have not recruited and trained enough cyber personnel to fill 133 teams. As an Army colonel noted, "The lack of talented personnel to fill the positions on the teams has been and continues to be a severely limiting factor for the overall force. From the onset of U.S. Cyber Command, [the] services focused on recruiting, retaining, and filling teams to reach fully operational capable (FOC) status. Once teams achieve FOC, they often filled between 67-75 percent capacity." As a result, teams that are officially considered to be FOC are not, in reality, at 100 percent strength.

4/23/24, 12:48 PM

United States Cyber Force

According to multiple interviewees, proficient cyber operators are double-counted to make it appear like all the teams are at full strength. The services "play a shell game [with their] top tier talent," one Army major warned. "It is a common occurrence that the same 50 people are constantly task-organized from across the force to solve any and all of the command's hardest problems." An Army captain gave a similar account of how his service initially brought its cyber teams up to FOC: "The Army's rush to get teams to Full Operational Capability (FOC) was built on a farcical shell game in which the same personnel were moved from recently certified teams to new teams until all teams had certified. Yet few are able to provide capability if asked."

An Army Reserve major similarly said that U.S. Army Cyber Command "consistently bent numbers, changed interpretations, and moved soldiers from team to team, or mission element to mission element, to paint the picture that teams were both fully manned and fully trained." In fact, the officer said, "most [Cyber Protection Teams] never exceeded 75 percent of their intended manning and relied on a core squad of fully trained people cleverly assigned to launder the reality that most soldiers were not fully trained." This deception "was compounded by unrealistic training timelines." U.S. Army Cyber Command "issued demanding deadlines to reach FOC, and lower-level commanders would then force timelines to move even faster — presumably to maximize their personal performance evaluations." The result was an "environment that incentivized exaggerating how many soldiers and [Cyber Protection Teams] were FOC and disguising our numbers to higher headquarters."

Acquisitions Challenges

Across the U.S. military, it takes an average of 10 to 15 years to field a new capability.⁷⁹ Yet in the cyber domain, tools are frequently updated and rendered obsolete within a year or two of development (if not sooner). Nevertheless, the services continue to enjoy a preponderant share of the budget and acquisitions authority for cyberspace even though they have not adapted to meet CYBERCOM's timeline for tool acquisition. Thus, CYBERCOM is stuck with out-of-date capabilities and is forced to borrow the NSA's tools, explaining why assessments continue to conclude that severing CYBERCOM from the NSA would have detrimental effects.

Recognizing this problem, Congress has intervened several times to grant CYBERCOM greater control over the acquisition of capabilities, resulting in incremental changes to ameliorate this issue. However, this solution runs contrary to civilian oversight of acquisition, which services have and CYBERCOM does not.

In the FY 2016 NDAA, Congress granted CYBERCOM authority for the development, acquisition, and sustainment of cyber-specific equipment and capabilities.⁸⁰ The following year, Congress amended DoD's special emergency procurement authority to facilitate defense against and recovery from a cyberattack.⁸¹ As a result of more recent congressional direction, CYBERCOM in 2027 will assume "service-like acquisition decision authority" over platforms that the command uses to conduct cyber operations.⁸²

Since the passage of the FY 2016 NDAA, CYBERCOM has been able to hire some acquisition professionals, but it continues to outsource most contracting, as the services make the large purchases on its behalf.⁸³ The director of CYBERCOM's acquisitions directorate said that since Congress granted the command EBC, he hoped to hire 40 people in 2023 and up to another 50 in 2024. But this is still a fraction of the personnel required to manage a \$3 billion budget. In comparison, the Army boasts that its acquisition workforce "is composed of approximately 32,000 civilian and military professionals,"⁸⁴ or about one person for every \$6 million of discretionary budget.

Despite CYBERCOM's acquisition authorities and EBC, the lion's share of funding for cyberspace activities remains with the services. The services, however, lack a unified process for spending money on cyber-related capabilities, equipment, training, and education. This leads to redundant and disparate efforts, not effective preparation for joint warfighting. As a major in the U.S. Air Force noted, "The services and the other combatant commands have taken it upon themselves to acquire their own cyber capabilities to meet their needs, resulting in vast duplication and reliance on defense contractors to provide questionable and often self-serving operational guidance."

Another Air Force major similarly shared:

I've witnessed vendors sell the same \$100M offering to two services under a different name so those services could independently lobby for resources. I've witnessed one service sabotage another's cyber operation (both under the same Joint Force Headquarters) simply because that service did not receive credit. I've seen the services' acquisition communities spend over \$1B on poorly defined and duplicative cyber requirements to deliver tools that will never be used. Every effort to unify resources and address national priorities is undermined and resisted by the services who perceive no benefit to their domains.

All of this ultimately reduces force readiness. Without the correct equipment, even the best-trained cyber warrior cannot be effective in conflict. Moreover, the ongoing effort to transfer acquisition authority to CYBERCOM, while borne out of a legitimate frustration with the status quo, will result in the removal of traditional civilian oversight of acquisition, which only the services can provide.

Counterarguments to Establishing a U.S. Cyber Force

Some experts who acknowledge the force-generation challenges facing CYBERCOM nevertheless oppose the creation of a Cyber Force.⁸⁵ They offer four main arguments against creating an independent, uniformed cyber service.

Counterargument 1: A Cyber Force will negatively impact readiness in the short term and create budgeting and personnel problems for the other services.

This critique posits that creating a Cyber Force would deprive the services of critical personnel. Transferring capable IT and cybersecurity professionals now focused on network architecture and the defense of internal service systems to the Cyber Force would leave the services bereft of skilled personnel. However, shifting only CMF billets, which do not include the services' IT and cybersecurity personnel, would render this potential issue moot.

A related objection argues that transitioning personnel and budgets to the Cyber Force from multiple services would impose an insurmountable administrative burden. Prior to the establishment of the Space Force, the preponderance of space-related personnel and investments were already housed within the Department of the Air Force. But cyber-focused personnel and funding are currently much more dispersed.⁸⁶ While this is true, all services have existing methods for inter-service transfers. By streamlining these transfers, the Space Force acquired more than 13,000 servicemembers and civilians in its first two years.⁸⁷

Counterargument 2: The Space Force should be responsible for force generation for cyberspace.

Some commentators argue that DoD should combine cyber and space operations under the control of the Space Force. Those who favor this position tend to believe a service's value is based at least in part on its size. At present, the Space Force is small but set to grow from 8,400 to 16,000 uniformed and civilian Guardians and may continue to grow based on the importance of space operations.⁸⁸ More to the point, however, this critique ignores the fact that a small number of highly skilled operatives can be effective in cyberspace.

The argument also presumes an inherent link between space and cyberspace. Space assets, such as communications satellites, indeed serve a critical function in the transmission of information. Likewise, many ground operations and weapons systems are also dependent on space assets, but this does not mean the Space Force should train personnel for ground operations. As distinct operational domains, space and cyberspace have unique "man, train, and equip" requirements.

Counterargument 3: The SOCOM model is a better fit for cyberspace than a Cyber Force.

Perhaps the most common counterargument to the creation of a Cyber Force is that CYBERCOM should apply the SOCOM model to cyberspace—notwithstanding SOCOM's own growing pains over its 30-year history.⁸⁹ However, while SOCOM and CYBERCOM both possess highly skilled operators, they are otherwise very different.

In the SOCOM model, each of the services provides the force employer—SOCOM—with expert personnel who possess skills suited to their particular domain. For instance, an Army Ranger trains for special operations on land, while Navy SEALs possess skills tailored to maritime special operations. Rangers and SEALs are not interchangeable. The Army cannot train SEALs, nor the Navy Rangers. Thus, SOCOM actually gains strength from this one-of-a-kind distributed force-generation model.

However, there are no land, sea, or air-specific cyber functions that only particular services can provide. As one U.S. Navy captain noted, SOCOM's "success is achieved by allowing each of the service-specific commands to specialize in discrete types of warfare, technologies, and operational environments." By contrast, as a retired Navy captain noted, "Cyberattacks will not be, nor are they currently, service-specific nor sector-specific, so it does not make sense to have created service-specific mission teams, different designators, MOSs, etc., to respond to the broad scale of cyberattacks."

A side-by-side comparison of the SOCOM and CMF structures depicts two wholly different organizational architectures, as illustrated in figures 3 and 4. SOCOM's organization into many sub-unified commands and geographic commands does not reflect the requisite structure of CMF and its component parts.

4/23/24, 12:48 PM

United States Cyber Force

Figure 3: SOCOM Structures**Figure 4: CYBERCOM Structures**

SOCOM has also faced the same challenges as CYBERCOM regarding drawing personnel from disparate services. The services' inconsistent definitions of overlapping skill sets create incompatibility. This makes interoperability challenging, particularly in dynamic, high-operational-tempo environments. Although the defense community is largely content with the way SOCOM is organized, led, and operated, a GAO report from October 2022 noted that SOCOM has its own challenges concerning oversight and command and control.⁹⁰ For SOCOM, a dependence on multiple services makes some of these challenges unavoidable, yet the U.S. military has a better option for cyber force generation.

Counterargument 4: CYBERCOM should absorb many of the man, train, and equip responsibilities from the services.

Rather than creating a Cyber Force, some argue that CYBERCOM should evolve to absorb the force-generation responsibilities from the other services. This approach would be tantamount to carving out an exception for cyber-related military matters from the 1986 Goldwater-Nichols Act, the landmark legislation that drew the line between force generation and force employment.

In this scenario, the commander of CYBERCOM would become responsible for military cyber force generation and force employment in addition to his or her duties as head of the NSA. While the dual-hatted structure for CYBERCOM and the NSA was initially intended to be temporary, it remains advantageous, as concluded by a December 2022 study led by General (Ret.) Joseph Dunford, former chairman of the Joint Chiefs of Staff.⁹¹ The study, however, conceded that simultaneously leading both organizations is a significant amount of work for one individual. Adding what would effectively be a third hat — force-generation responsibilities — would leave the commander less time for the other two, or even force DoD to sever NSA from CYBERCOM.

<https://www.fdi.org/analysis/2024/03/25/united-states-cyber-force/>

13/22

What Should a Cyber Force Look Like?

Many of the challenges outlined in the section above could only be solved or at least significantly mitigated through the creation of the Cyber Force as the force generator for the cyber domain. CYBERCOM would remain the force employer. This new Cyber Force could be located within the Department of the Army, just as the Marine Corps is housed within the Department of the Navy and the Space Force sits within the Department of the Air Force.

Standing up this new service would be relatively straightforward. Initially, the Cyber Force would encompass the billets that currently comprise the CMF: a 6,200-person mission group consisting of servicemembers, civilians, and contractors (see Figure 5).⁹² Beyond the CMF, the Cyber Force could also absorb a select number of billets for cyberspace operators that currently fall within the SOCOM enterprise.

Figure 5: Initial Billets of a New Cyber Force

In addition, the Cyber Force would require the transfer (or addition) of support staff billets and infrastructure. The services would likely need to retain some cyber support staff, but a percentage of the cyber-specific force-generation billets from each of the services would transfer to the Cyber Force, particularly those necessary for Cyber Force training institutions. And some Cyber Force recruitment of existing servicemembers would be necessary to fill the remaining gaps in support staff. This shift, however, should not strain the resources of any one service. In total, the Cyber Force would probably initially comprise approximately 10,000 personnel, although this number would likely grow over time as cyber threats continue to expand.

The Cyber Force could draw on lessons from the Space Force, which has encountered few issues filling its new roles even though it requires highly technical and skilled personnel.⁹³ At a leadership level, the Space Force's establishment mostly required the lateral transfer of personnel from Air Force Space Command.⁹⁴ The Space Force, which currently has 8,400 billets, attributes much of its recruiting success to being small, agile, and selective with applicants. Its leaders understand they do not need to mimic the larger services.⁹⁵ To boost recruitment, the service has also taken advantage of opportunities for the direct commissioning of civilians with requisite skills for space.⁹⁶

Most importantly, the creation of a Cyber Force would not require an extensive or complex shuffle of personnel, and the services would retain defensive cyber personnel and IT infrastructure management capabilities for the DoD information networks (DODIN). The creation of a Cyber Force, however, would preclude service-retained personnel from conducting offensive cyberspace operations. Figure 6 illustrates proposed responsibilities of the Cyber Force and the services.

Figure 6: Proposed Responsibilities for the Cyber Force and the Services

An initial budget for the Cyber Force would be approximately \$16.5 billion, a fraction of the hundred-billion-dollar budgets of the Army, Navy, and Air Force. This estimate includes DoD's current allocation for the cyberspace activities budget (\$13.5 billion), minus the cybersecurity investments from the services (\$511 million). The budget estimate also includes the resources currently carved out for CYBERCOM under EBC (about \$2.9 billion), the military personnel funds (\$624.25 million), and training resources.⁹⁷ An apt comparison is the budget for the Space Force, for which DoD requested \$30 billion for FY 2024.⁹⁸

While the other services may see a slight reduction in their budgets after the creation of a Cyber Force, most of the decrease would come from a reduction in cyber force generation costs thanks to efficiencies from eliminating redundancies. The Cyber Force would consolidate the acquisitions process specifically for operational capabilities. It should not, however, become the IT and communications service provider for the services, a role that would distract it from operational priorities.⁹⁹

Creating a Cyber Force would also benefit the NSA.¹⁰⁰ A quarter of the NSA's workforce comprises active-duty military units, currently provided by the services. However, these units are not held accountable for successfully serving the NSA's mission. With a Cyber Force focused on delivering well-trained cyber personnel, the NSA would, in turn, receive more, high-quality, human resources.

During a visit to Navy Information Operations Command Pensacola, then deputy commander of U.S. Cyber Command Lt. Gen. Timothy Haugh, engaged in cyber discussions with Sailors on Oct. 12, 2023. (U.S. Navy photo by Petty Officer Third Class Leonell Domingo)

A Cyber Force would also facilitate the establishment of more robust legal principles for cyberspace. Military leaders and commanders have long required legal advisors for the specific domains in which they operate. The DoD legal community, in turn, has training, education, and experience tracks to develop attorneys who deliver this legal support. Yet unlike land, sea, air, and space, cyberspace is an interdependent global domain, entirely human-made, and consists largely of privately owned and operated systems. The current reliance on non-cyber lawyers serves U.S. cyber operations poorly.

If done properly, the overall readiness of the military's cyber forces should not suffer during a transition to an independent Cyber Force. Instead, cyber forces would gain more operational focus and direction while consolidating acquisition processes and maximizing budgetary effectiveness.

Conclusion

Years after designating cyberspace as a warfighting domain, leaders must acknowledge the writing on the wall. The scope and scale of cyber threats are growing. Cyberspace plays a central role in China's strategy as the "pacing threat" for the United States. China has already centralized its cyber, space, electronic warfare, and psychological warfare capabilities within its Strategic Support Force. Russia is actively leveraging cyber operations both on the battlefield and to threaten U.S. critical infrastructure and interfere in American politics.

Conventional wisdom holds that the U.S. military is well positioned to dominate in the cyber realm given CYBERCOM's current resources, capabilities, and authorities. However, recent congressionally mandated studies,¹⁰¹ independent analyses and audits, and the accumulated personal accounts from current and retired servicemembers demonstrate otherwise.

Previous attempts to increase U.S. cyber force readiness have failed. Measures such as the elevation of CYBERCOM to a unified combatant command, the promised expansion of the CMF, and the delivery of EBC do not address major underlying force-generation problems. U.S. policymakers must acknowledge the difficult reality that the military has tried and failed to salvage the status quo.

This failure stems from the basic fact that non-cyber services are responsible for cyber force generation. The solution is to create an independent, uniformed Cyber Force. While many experts have long called for the creation of an independent Cyber Force,¹⁰² policymakers should especially listen to the voices of those servicemembers with direct, extensive operational experience. The numerous first-hand accounts highlighted in this monograph offer a compelling testament to the need for an independent service for cyberspace.

The United States has a limited window of opportunity to reorganize, allocate resources, and develop sustainable cyber force readiness. The U.S. military has failed to fix the problem on its own. Only Congress can create a new independent service, so it is time for lawmakers to act.

Appendix A: Select Quotations from Interviews

The following are illustrative excerpts from more than 130 pages of interviews with 76 active-duty and recently separated servicemembers and Defense Department civilians about cyber readiness, CYBERCOM, and the challenges they have encountered. These interviews were collected over the course of the past year and speak to the significant challenges discussed throughout this monograph. The authors have chosen not to disclose the full remarks to protect the individuals who agreed to share their personal experiences.

Thirty-four percent of the interviewees came from the U.S. Army, 30 percent from the U.S. Navy, and 26 percent from the U.S. Air Force. A small number of accounts also came from the Marine Corps, Space Force, and DoD civilians. Most of the accounts (61 percent) came from officers with ranks of O-1 to O-6. Another 26 percent come from officers with ranks of O-3. Notably, one interview is with a general officer (O-7).

Figure 7: The Rank of Interviewees

Figure 8: The Service of Interviewees

General Officer, U.S. Military

"Our current strategy of relying on the existing Services to build the cyber expertise and capabilities required is inefficient, ineffective, and unlikely to succeed despite years of investment and the best efforts of our service members. Without a doubt, the only viable path forward for USCYBERCOM is to establish a new Service focused on organizing, training, and equipping forces required to fight — and win — in cyberspace."

"Years of investment and training are lost when service members are moved away from the cyber mission. Complicated and inconsistently applied incentive programs result in retention issues."

"Differences in training also impact USCYBERCOM's ability to conduct operations."

Colonel, United States Air Force

"In aggregate, we see a combatant command spending an inordinate amount of time executing Service-like responsibilities at the expense of its primary responsibilities to defend the [Department of Defense Information Networks], provide support to combatant commanders for execution of their missions around the world, and strengthen our nation's ability to withstand and respond to cyber-attack. Instead, we have a Department of Defense with no single service incentivized to put cyberspace operations at the forefront."

"If you look [at] who leads cyberspace operations in the Department of Defense, they are not typically grown from within the cyberspace operations force. Cyber leaders should lead cyberspace operations and represent cyberspace operations in joint warfighting. We need 'cyber minded' leaders."

Colonel, United States Army

"Having been on both the inside and outside of the Cyber Mission Force since it was first established, the lack of talented personnel to fill the positions on both teams has been and continues to be a severely limiting factor for the overall force."

"In fact, it was once found that about 10% of the personnel execute as much as 80% of the operational missions."

[On the subject of officers sitting on promotion boards] "Officers with advanced, skilled degrees in computer science from esteemed institutions are equated with those who received online degrees in information management; they are given no additional consideration for their knowledge, skills, or abilities and are disadvantaged. This is akin to equating a brain surgeon with a field medic."

Captain (Ret.), United States Navy

"The development of service-specific cyber specialty fields without dedicated senior level commitments has yielded varying levels of fragmented support to cyber operations, lack of continuity of cyber personnel, unclear career paths, insufficient experience, wide use of noncyber personnel in cyber leadership positions, and cyber operations being treated always as a supporting entity across all services."

"[C]yber attacks will not be nor are they currently service-specific nor sector-specific, so it does not make sense to have created service-specific mission teams, different designators, MOSs, etc., to respond to the broad scale of cyber attacks."

4/23/24, 12:48 PM

United States Cyber Force

Captain, United States Navy

"[United States Special Operations Command]'s success is achieved by allowing each of the service specific commands to specialize in discrete types of warfare, technologies, and operational environments. USSOCOM picks the 'best athlete' depending on the operational outcome they are trying to achieve."

"USCYBERCOM assigns the military services ... essentially requiring every team to master every aspect of cyber warfare to successfully operate against their assigned target. This methodology is completely out of sync with the way the rest of the DoD is constructed ... Applying the USCYBERCOM methodology to air warfare would be akin to requiring every service to operate the same aircraft, to accomplish every aspect of air warfare, in every operational environment."

Captain, United States Marine Corps

"Leading in the cyberspace domain demands technical competency that cannot be taught in a twelve-month schoolhouse alone. One of my worst professional experiences involved working underneath a woefully unprepared commander with a degree in culinary arts ... Under no circumstances would a cyber officer be asked to lead a squadron of aircraft, and yet the opposite is often true."

Major, United States Air Force

"I've witnessed vendors sell the same \$100M offering to two services under a different name so those services could independently lobby for resources. I've witnessed one service sabotage another's cyber operation (both under the same Joint Force Headquarters) simply because that service did not receive credit. I've seen the services' acquisition communities spend over \$1B on poorly defined and duplicative cyber requirements to deliver tools that will never be used. Every effort to unify resources and address national priorities is undermined and resisted by the services who perceive no benefit to their domains."

Colonel (Ret.), United States Army

"I've seen senior warfighting leaders dismissively call cyber research 'book reports,' cyber operators 'herds,' and cyber capability development 'science projects.' These ... leaders who make critical cyber operational, resource allocation, and risk assessment decisions control promotions to choose people that look like themselves."

Lieutenant Colonel, United States Marine Corps

"I can't speak for the other services, but I perceive a lack of career progression for cyber officers in the Marine Corps. I commanded a Combat Mission Team and am fully qualified to join the cyber field but decided not to apply for the specialty because of the limited command opportunities."

Lieutenant Colonel, United States Air Force

"[Headquarters, Air Force] has commissioned multiple RAND studies on cyber force structure, then ignores the key recommendations."

"Few, if any, qualified offensive cyber operators have graduated to positions of command, Colonels, and Generals. This is comparable to an Air Force in which none of the Colonels and Generals have ever been qualified pilots."

"Coupling Goldwater-Nichols and the fact that the USAF doesn't see 'cyberspace operations' as one of its core missions, [the U.S. Air Force] will likely continue to deprioritize developing and promoting leaders to achieve DoD objectives in and through cyberspace." [USAF removed "cyber" from the Air Force Mission Statement in 2021.]

Captain, United States Air Force

"Not for more money or flexibility—I always understood the military couldn't match industry here, but that's not why anybody I knew joined the military. I left for the same reason as many others: when you feel your organization keeps you from making an impact on the mission and you can't change the organization, then you either have to stop caring so much or leave. I saw two primary things holding the Air Force back that it would not fix. I believe it will require a separate cyber service to address these problems: One, organizationally the Air Force lacks understanding of the cyber domain, and, two, it has failed to take cyberspace operations seriously as a warfighting discipline."

"During my career, I learned that making cyber operations look like the rest of the Air Force was more important than mission success. For the sake of the mission and the people, we need a separate cyber service and we must understand that lives depend on operational success in cyberspace. A general once told me 'Someday you can change things; when you're a general.' They didn't know what that

4/23/24, 12:48 PM

United States Cyber Force

really communicated to me."

Commander, United States Navy

"The core of the issue facing the broader [Cyberspace Operations Forces] is the lack of a single service designed to man, train, equip, and manage the careers of a full cadre of Cyber Operations professionals. The current construct of the military services is not conducive to developing, retaining, and advancing a highly trained Cyber Force. Each service is focused on being proficient in and advancing those servicemembers who excel in their respective warfighting domains (sea, air, and land)."

Captain, United States Army

"It is important to highlight the issues in Cyber are not solely because of problems within the Army. A lack of joint command vision regarding the separation of roles and responsibilities between USCC and the NSA, for example, has led to significant confusion and constantly changing direction regarding what problems the command is required to solve."

Major, United States Air Force

"In short, the Air Force values breadth over technical depth and meeting requirements on paper versus building and enabling true technical talent. When I arrived at Keesler AFB for my initial skills training as a cyber warfare officer, I was ecstatic. I was finally going to be a part of the force responsible for the slogan 'It's not science fiction, it's what we do every day.' I expected training and equipment that would enable me to contribute to homeland defense or project power in current conflicts around the globe. The reality was very basic training which was worse than most industry offerings and equipment worse than what I had purchased for myself to use at home. Additionally, the training itself was disjointed and lacked focus—covering everything from space-based platforms to loading pallets with only a few weeks of actual offensive or defensive cyber training."

Appendix B: Historical Case Studies: The Air Force and Space Force

In the past, when the DoD has faced force-generation or force-employment challenges, the U.S. military has undergone significant reorganization.

World War I firmly demonstrated the ability of aircraft to "impact an enemy beyond a depth that could be readily imagined by those operating in [land and sea]."¹⁰³ After the war, the War Department (the predecessor to DoD) and congressional leaders began to evaluate the implications of flying for future military operations and subsequently renamed the Air Service the U.S. Army Air Corps. While the Corps was not an independent service, it "strengthen[ed] the conception of military aviation as an offensive, striking arm rather than an auxiliary Service."¹⁰⁴ Each service began investing in its own aviation capabilities.

During the interwar period, multiple boards examined the country's readiness for, and resources dedicated to, military flying missions. Most notably, the 1919 Menoher Board found the "best way to take advantage of the new technology in aviation was to create a new military organization."¹⁰⁵

By the end of World War II, air power had emerged as a pivotal force, affirming the wisdom of the Menoher Board's recommendation. The National Security Act of 1947 established the U.S. Air Force as an independent, uniformed service, 30 years after Congress began documenting officers raising that the domain could not be effectively handled by the compartmentalized efforts of the U.S. Army and U.S. Navy.

In 1982, the Air Force established the first Air Force Space Command. In 1985, the United States established a unified U.S. Space Command,¹⁰⁶ tasked with coordinating Army, Naval, and Air Force space forces and providing "space-based missile warning, communications, navigation, weather, and imagery capabilities."¹⁰⁷ The 2001 Rumsfeld Commission first proposed the establishment of a Space Force.¹⁰⁸ But a year later, DoD disbanded the U.S. Space Command and gave its responsibilities to U.S. Strategic Command.¹⁰⁹

Over the next 16 years, however, DoD leaders began to recognize that no one military entity was placing sufficient emphasis on space security. China's demonstration of its anti-satellite capabilities, along with other threats, ignited conversations among policymakers that mirrored those prior to the establishment of the Air Force.¹¹⁰ DoD leaders also began realizing that U.S. Strategic Command's responsibilities were becoming "too big for one combatant commander to manage."¹¹¹

In 2008, Congress commissioned the Institute for Defense Analyses to write a report on "Leadership, Management, and Organization for National Security Space." It highlighted the need for a greater number of operators who are "steeped in space."¹¹² Over the next decade, the U.S. military increased its capabilities in space and focused on specializing organizational, acquisitions, and personnel training structures.

4/23/24, 12:48 PM

United States Cyber Force

In December 2018, President Donald Trump signed an executive order authorizing DoD to reinstate U.S. Space Command as a unified combatant command responsible for force employment in space. In the FY 2020 NDAA, Congress then established an independent U.S. Space Force to man, train, and equip personnel for U.S. Space Command. Articulating the connection between these two entities, then commander of U.S. Space Command Air Force Gen. John "Jay" Raymond noted, "U.S. Space Command will only be as strong as the capabilities it is provided by the United States Space Force."¹¹³

Ultimately, it took congressional intervention to establish independent uniformed services for air and space. Congressional intervention is again needed to address the significant readiness challenges stemming from the current organization and structure of U.S. cyber forces.

Figure 9: The Space Force vs. Space Command

Appendix C: The History of U.S. Information Operations and the Creation of CYBERCOM

The concept of "cyber" in the military lexicon did not appear until well after the military established doctrinal concepts for information operations, psychological operations, and computer network operations (both offensive and defensive).¹¹⁴ Information and psychological operations have been around for centuries, long predating wired and wireless communications. The notion that computer networks could multiply the effects of these operations, however, began to take hold in the late 1980s and 1990s. As DoD became more dependent on information systems for command and control, it created the Joint Task Force-Computer Network Defense. After the Gulf War, during which the U.S. military exploited technological advantages to ensure fast, efficient battlefield victories,¹¹⁵ the task force evolved into the Joint Task Force-Computer Network Operations (JTF-CNO).¹¹⁶

4/23/24, 12:48 PM

United States Cyber Force

The U.S. military began developing cyber doctrine in earnest in 2003 following the discovery of "Moonlight Maze," a multi-year Russian cyber espionage operation against U.S. systems. This campaign, which stole sensitive documents from U.S. government agencies, marked the "first large-scale cyberespionage attack by a well-funded and well-organized state actor."¹¹⁷ The next year, the Joint Chiefs of Staff defined cyberspace as a warfighting domain.¹¹⁸ DoD released its first National Military Strategy for Cyberspace Operations in 2006.¹¹⁹

Two years prior to that strategy's release, DoD reorganized JTF-CNO under U.S. Strategic Command. The Joint Task Force-Global Network Operations (JTF-GNO) handled cyber defense, and the Joint Functional Component Command-Network Warfare (JFCC-NW) handled offensive missions. However, after additional significant cyber espionage campaigns by U.S. adversaries, DoD combined the two and established CYBERCOM as a sub-unified combatant command under U.S. Strategic Command in 2010, led by a commander dual-hatted as the director of NSA. CYBERCOM was tasked with "direct[ing], synchroniz[ing], and coordinat[ing] cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners" as well as defending DoD information systems and the nation from significant cyberattacks.¹²⁰

CYBERCOM inherited the missions of defending DoD information systems, supporting joint force commanders in cyberspace, and advancing national interests in and through cyberspace. The services became responsible for force generation and force development. They also developed their own components responsible for information and cyber operations in support of operations in their respective warfighting domains.

In 2018, the president ordered the elevation of CYBERCOM to a unified combatant command. Compared to a sub-unified command, each unified combatant command has additional support mechanisms, a direct line of communication to the secretary of defense through a four-star general, greater authority to request budgetary resources, and a distinct geographical or functional responsibility.¹²¹ CYBERCOM also has dedicated combatant command staff, mirroring the organizational structure of the Joint Staff at the Pentagon.

In parallel, CYBERCOM gained additional authorities to conduct military cyberspace operations short of armed conflict to persistently engage and contest adversaries outside of DoD-controlled cyberspace. In FY 2012, the NDAA affirmed that DoD can conduct offensive operations in cyberspace "subject to the ... legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict and the War Powers Resolution."¹²²

The FY 2019 NDAA stated that clandestine cyber operations may be launched short of hostilities. The law also gave DoD the authority "to take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter" in response to "an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempting to influence American elections and democratic political processes." The law further authorized CYBERCOM to disrupt and respond to attacks in cyberspace, redefining cyber as a "traditional military activity."¹²³

These new authorities largely aligned with the Trump administration's National Security Presidential Memorandum-13, which officials say streamlined the process for authorizing military cyber operations.¹²⁴ These changes also coincided with CYBERCOM's publication of its first command vision, "Achieve and Maintain Cyberspace Superiority," as well as DoD's release of the 2018 DoD Cyber Strategy.¹²⁵

Finally, in the FY 2022 NDAA, Congress granted CYBERCOM Enhanced Budgetary Control (EBC). These authorities will take full effect in 2024, allowing CYBERCOM to directly control resources for equipping the Cyber Mission Force.¹²⁶ As General Paul Nakasone testified to Congress in March 2023, the objective is to better harmonize CYBERCOM's responsibilities and cyberspace operations by providing the command with control over funding for major acquisition programs that the services were previously directing. In anticipation of these responsibilities, CYBERCOM has stood up a joint cyber weapons program management office.¹²⁷

In 2022, the secretary of defense elevated the CNMF (within CYBERCOM) to a sub-unified combatant command, providing it with additional authorities and responsibilities. After more than a decade, CYBERCOM now has the Traditional Military Activities authority to conduct overt and clandestine action in support of U.S. armed conflict.¹²⁸ CYBERCOM also has acquisition authority and statutory responsibility for managing its personnel.

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

APRIL 10, 2024

QUESTIONS SUBMITTED BY MRS. MCCLAIN

Mrs. MCCLAIN. One of the trends we are seeing in terms of cyber-attacks is that adversaries have figured out how to phish many of the legacy tools that we have used in authentication. Not just passwords, but also some of the tools that we have used in multi-factor authentication (MFA), such as one-time passwords and push notifications. Civilian agencies seem to be making good progress on this front, thanks in large part to a 2022 OMB memo (M-22-09) that required agencies to use only “phishing-resistant authentication” that can block phishing attacks; CISA and NIST have also been highlighting the importance of phishing-resistant authentication, such as products that use the FIDO standards, to civilian agencies in their guidance.

As OMB noted, users can be fooled into providing a one-time code or responding to a security prompt that grants the attacker account access, and these attacks can be fully automated and operate cheaply at significant scale. But there is no similar policy in DOD to ensure that, in places where the Common Access Card (CAC) and its PKI authentication can’t be used, the authentication tools that are being used can block phishing attacks.

Can you explain why DOD seems to be behind civilian agencies on this critical cybersecurity control (ensuring that phishable authentication can no longer be used)?

What are your plans to close this security hole across the Defense Department? Will the DOD create a strategy or policy to ensure that whenever the CAC can’t be used, any alternative authenticator can block phishing attacks?

Ms. MANNING. The cyber threat landscape is evolving at a pace that requires a coordinated, agile, and defensive response. I applaud the efforts of CISA and NIST to prioritize phishing-resistant multi-factor authentication (MFA) within civilian agencies. Phishing-resistant MFA and Zero Trust security architectures are critical requirements for all federal agencies, per Executive Order 14028 on improving the Nation’s cybersecurity. The DoD Chief Information Officer (CIO) has prioritized implementing Zero Trust through continuous multi-factor authentication, micro-segmentation, advanced encryption, endpoint security, analytics, and robust auditing among other capabilities to fortify data, applications, assets, and services to deliver cyber resiliency. It is DoD policy that organizations use the Common Access Card (CAC) as the authenticator of choice wherever possible, including cloud environments. In scenarios where a CAC cannot be used or the user does not have a CAC, DoD has a list of approved phishing-resistant authenticators for which the user’s identity is tied to a hardware device. The DoD CIO is currently working with the components to develop a DoD MFA strategy that will guide the use and approval of anti-phishing MFAs when use of the CAC is not possible.

Mrs. McCLAIN. Last May, the DOD CIO put out a policy (DOD Instruction 8520.03, "Identity Authentication for Information Systems" that created a formal approval process for multi-factor authentication (MFA) technologies to be used as an alternative to the Common Access Card (CAC) and its PKI-based authentication, with a focus on ensuring that strong MFA is being used in applications which cannot easily integrate with the CAC or where the use of PKI is not practical. For example, the CAC is not optimized for use in some mobile devices. In addition, a CAC is not issued to every individual that requires access to DOD resources.

Can you share how many MFA solutions have been approved under this new policy? And have any of these approvals been for phishing-resistant authentication solutions that can block the increased volume of phishing attacks that have been targeting legacy MFA technologies such as one-time passwords and push notifications? What can be done to accelerate this process?

Ms. MANNING. Four alternatives to the DoD Common Access Card (CAC) have been approved under DoD Instruction 8520.03, "Identity Authentication for Information Systems," two of which are phishing-resistant. The other two multi-factor authentication (MFA) technologies were approved prior to the release of the updated DoD Instruction. Another five alternatives are being evaluated. Of the ones currently being evaluated, all are intended to be phishing-resistant. DoD is developing an MFA strategy that will inform an update to DoDI 8520.03 and guide the selection and use of alternative MFAs.

Mrs. McCLAIN. One of the trends we are seeing in terms of cyber-attacks is that adversaries have figured out how to phish many of the legacy tools that we have used in authentication. Not just passwords, but also some of the tools that we have used in multi-factor authentication (MFA), such as one-time passwords and push notifications. Civilian agencies seem to be making good progress on this front, thanks in large part to a 2022 OMB memo (M-22-09) that required agencies to use only "phishing-resistant authentication" that can block phishing attacks; CISA and NIST have also been highlighting the importance of phishing-resistant authentication, such as products that use the FIDO standards, to civilian agencies in their guidance.

As OMB noted, users can be fooled into providing a one-time code or responding to a security prompt that grants the attacker account access, and these attacks can be fully automated and operate cheaply at significant scale. But there is no similar policy in DOD to ensure that, in places where the Common Access Card (CAC) and its PKI authentication can't be used, the authentication tools that are being used can block phishing attacks.

Can you explain why DOD seems to be behind civilian agencies on this critical cybersecurity control (ensuring that phishable authentication can no longer be used)?

What are your plans to close this security hole across the Defense Department? Will the DOD create a strategy or policy to ensure that whenever the CAC can't be used, any alternative authenticator can block phishing attacks?

General HAUGH. The DOD CIO, as the author of the DoD Instruction 8520.03, "Identity Authentication for Information Sys-

tems,” published on May 19, 2023 and DoD Instruction 8520.02, “Public Key Infrastructure (PKI) and Public Key (PK) Enabling,” published on May 24, 2011, is best postured to provide a formal response regarding the perception of an authentication security hole and any efforts to address them with strategy or policy. As the policy owner, DOD CIO “Approves [multi-factor technology] MFA technologies for use by DOD information systems . . .” while also addressing applicable security controls. JFHQ–DODIN, on behalf of USCYBERCOM, manages cyberspace risk to DoD missions by executing command and control across all DoD components and reinforcing or augmenting DoD policy whenever practical through the release of operational orders. In this role, JFHQ–DODIN is responsible for synchronizing and coordinating actions in and through cyberspace so that the Department remains postured against sustained threats posing risk to the nation’s strategic interests. Operational orders may be proactive or preventative in nature, may be focused on availability and resiliency of the DODIN, or may be responsive to suspicious or malicious events. All orders, regardless of focus, are tracked to completion and subsequently monitored for compliance.

Mrs. MCCLAIN. Last May, the DOD CIO put out a policy (DOD Instruction 8520.03, “Identity Authentication for Information Systems” that created a formal approval process for multi-factor authentication (MFA) technologies to be used as an alternative to the Common Access Card (CAC) and its PKI-based authentication, with a focus on ensuring that strong MFA is being used in applications which cannot easily integrate with the CAC or where the use of PKI is not practical. For example, the CAC is not optimized for use in some mobile devices. In addition, a CAC is not issued to every individual that requires access to DOD resources.

Can you share how many MFA solutions have been approved under this new policy? And have any of these approvals been for phishing-resistant authentication solutions that can block the increased volume of phishing attacks that have been targeting legacy MFA technologies such as one-time passwords and push notifications? What can be done to accelerate this process?

General HAUGH. The DOD CIO, as the author of the DoD Instruction 8520.03, “Identity Authentication for Information Systems,” published on May 19, 2023 and DoD Instruction 8520.02, “Public Key Infrastructure (PKI) and Public Key (PK) Enabling,” published on May 24, 2011, is best postured to provide a formal response. As the policy owner, DOD CIO “Approves [multi-factor technology] MFA technologies for use by DOD information systems . . .” and is therefore the appropriate source of MFA solution approvals and other process-related questions.

QUESTIONS SUBMITTED BY MR. LALOTA

Mr. LALOTA. How is DoD tracking cyber workforce training, credentials, and job placements?

Ms. MANNING. The Department has a robust overarching governance architecture for managing the training, credentialing, and assignment of its 230,000-person cyber workforce. This architecture is defined in DoDD 8140.01 “Cyberspace Workforce Management,”

which established the Cyberspace Workforce Management Board (CWMB) as the governing body tri-chaired by the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), the DoD Chief Information Officer (CIO), and the Principal Cyber Advisor (PCA). The DoDD 8140.01 specifies the DoD Cyber Workforce Framework (DCWF), comprising 72 cyber-related work roles, as the basis for cyber workforce identification (e.g., assigning work roles to military and civilian positions) and qualification requirements (e.g., education, training, certifications, job-specific credentials) tailored to each work role's basic, intermediate, and advanced proficiency levels.

Work role categorization allows the CWMB to make more targeted decisions with respect to hiring, retention, and incentives based on the criticality of various roles. The Services and DoD agencies maintain their own qualification tracking systems with unique data constructs. For example, USCYBERCOM tracks training and credentials of the Cyber Mission Force in its Joint Cyber Command and Control-Readiness system (JCC2R). The DoD CIO launched a data maturity initiative in FY 2024 to generate a holistic assessment of cyber workforce readiness garnering qualification metrics across DoD. During the first phase of this effort, the DoD CIO conducted an environmental scan of DoD workforce tracking systems which identified authoritative sources to harness qualification data. The second phase underway involves creating data structure and standardization to enable integration of qualification data from DoD's disparate systems. The DoD CIO currently employs Advana, DoD's data analytics platform, for tracking cyber workforce work role identification through dashboards and other data visualization and plans to leverage automated tracking and reporting of cyber qualifications utilizing Advana in FY 2026.

Mr. LALOTA. What steps are CYBERCOM and the DOD taking to cultivate and support the development of cyber talent within the defense industry?

General HAUGH. USCYBERCOM continues to pursue additional authorities to maximize our ability to recruit and retain high demand, low-density cyber talent across the global cyber enterprise to better enable us to fight and WIN the war for talent. J1 is collaborating with DoD CIO, the Principal Cyber Advisor, and OSD Policy to execute NDAA 1531 to incentivize our service members with up to \$2500 bonus for their novel action, invention, or achievement that enables operational outcomes in cyberspace against threats to National Security. Additionally, we are advocating for Target Local Market Supplement (TLMS) pay for our critical work roles with high turnover rates to increase pay up to ~28%.

Lastly, we are partnering with Army to execute the 10 U.S.C. 4092 authorities to hire imminent experts in data science, computer science, and computer network exploitation and pay them above the GG pay scale (\$181K—246K annually, with the ability to incentivize up to 25% of base pay). This could result in an annual pay in upwards of \$307K. USCYBERCOM continues to maximize the use of our Cyber Excepted Service authorities while pursuing the additional authorities outlined above, which refine the Command's ability to engage talent through partnerships and innovation and allow further competition with industry salaries. Mov-

ing forward, we recognize the Campaign for Talent goes beyond financial incentives and requires a holistic approach to recruit AND retain world-class talent we need to support the cyber enterprise. USCYBERCOM stood up a Civilian Workforce Council, charged with identifying development and mentorship opportunities for the military and civilian workforce to set us apart from the competition and intentionally grow talent to fill key positions within the broader cyber enterprise. We are expanding our internship opportunities and collaborating with our Academic Engagement Network (AEN) of 127 schools, to inspire the next generation of cyber talent.

Through the AEN, the Command has direct access to the students and faculty at these schools, establishing a pathway for students to seek employment at USCYBERCOM or other government agencies in the cyber field. Finally, our Command Code is, “We WIN With People.” Our new cyber recruiting cell enables global recruiting in support of the cyber mission and affords us the opportunity to rapidly identify and recruit the talent we need to enable our mission in defense of the Nation. Speed and agility is the key to our success.

Mr. LALOTA. Are there particular programs or partnerships in place to ensure that even small and medium-sized defense suppliers, like the strong core of defense industrial suppliers on Long Island, have access to skilled cybersecurity professionals to meet the strategy’s compliance requirements and enhance their cyber posture against the backdrop of evolving cyber threats?

General HAUGH. NSA’s Directorate of Cybersecurity operates the Cybersecurity Collaboration Center (CCC). The CCC operates a Defense Industrial Base (DIB) Defense program that supports enhanced security of the DIB by providing intel-driven cybersecurity solutions to DoD contractors (to include small and medium sized defense suppliers). DIB Defense (NSA C53) provides cybersecurity services that address the top ways nation-state actors target the DIB, and are infused with NSA’s unique insights and analytics. These services include Protective Domain Name System (PDNS), Attack Surface Management (ASM), and Threat Intelligence Collaboration (TIC).

In addition to these core services, DIB Defense also runs multiple pilot services with DIB partners to include Cloud Security, Threat Hunting, Phishing Protection, and Autonomous Penetration Testing. UNDERADVICE (UNAD) is a Cyber National Mission Force (CNMF)-designated information-sharing activity designed for partnerships with private sector entities. This information sharing is overt, voluntary, and reciprocal, with acknowledgement of the identities of the participants and the organizations to which they belong. This allows for appropriate information sharing regarding cybersecurity and cyber threats related to assigned missions between CNMF and the private sector. UNAD complements other USG information sharing programs, complies with existing U.S. law and policy, and allows for engagement with the private sector on terms with which the private sector is accustomed.

CNMF information sharing under UNAD facilitates CNMF operations and timely partner defensive actions. Currently, UNAD is an unfunded activity but will be designated as the USCYBERCOM Executive Agent responsible for managing cyber threat information

sharing between USCYBERCOM Components and the private sector to meet the intent of FY19 NDAA § 1642(b) and FY22 NDAA § 1508. Outside of USCYBERCOM, the Cybersecurity and Infrastructure Security Agency (CISA) ensures members of the Defense Industrial Base (DIB) have access to skilled cybersecurity professionals to enhance their cyber posture against the backdrop of evolving cyber threats. Specifically targeted to supporting the DIB, CISA manages the DoD's Defense Industrial Base Cyber Program specifically seeking to enhance and supplement DIB participant's capabilities to safeguard DoD information that resides on or is transmitted on unclassified information systems. This program is free of cost to DIB participants and open to all cleared defense contractors. For more information, potential DIB participants should reach out to CISA at OSD.DIBCISA@mail.mil or visit their website at <https://DIBNet.dod.mil>.

QUESTIONS SUBMITTED BY MR. WITTMAN

Mr. WITTMAN. The threat of Chinese cyber capabilities continues to be a persistent and penetrating issue for the Congress and U.S. Government in general. One of the vulnerabilities that Congress continues to address is TikTok. The Congress took action and banned TikTok on all government devices and devices that access government information. Given the young age of many service members, it is not presumptuous to assume that many of them have TikTok accounts and have downloaded the application on their personal devices. To protect the data of U.S. service members, personally identifiable information, and controlled and classified information, is the Department of Defense currently compliance with US Code S.1143—No TikTok on Government Devices Act? What is the Department doing to ensure that the TikTok ban is enforced, particularly on Government issues cell phones or any bring your own device solutions. Finally, how does the Department intend to enforce this Code with the contractors required and identified under CMMC guidance?

Ms. MANNING. TikTok remains a national security concern due to the sheer volume of user data it collects and potential for exposure and access of U.S. user data by PRC-based ByteDance. It is crucial for our Nation to tackle this issue, especially as similar applications will arise, requiring policies that strike a balance between information access and protection against adversarial surveillance and malign influence. On March 3, 2023, the DoD Chief Information Officer (CIO) released the "Removal and Ban of the Installation of TikTok" and provided implementation guidance on May 4, 2023. Both memoranda enforce the TikTok ban on all government devices. DoD policy required removal of the TikTok application from all government devices. Furthermore, the "DoD Mobile Device Policy" and "Use of Non-Government Owned Mobile Devices" policy requires government and contractor issued devices to be enrolled in an Enterprise Mobility Manager (EMM) for management of DoD information and applications. Once enrolled, managed devices can only install mobile applications that have been approved by the EMM and are available through the managed appli-

cation store. This requirement ensures the TikTok ban is enforced on all government devices.

Moreover, the Cybersecurity Maturity Model Certification (CMMC) Program will require that DoD contractors manifest compliance with the cybersecurity safeguards in already required standards as a condition of receiving awards and continued business. The purpose of the CMMC Program is to validate that existing security requirements in NIST Special Publication (SP) 800–171, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations” and select security requirements from NIST SP 800–172, “Enhanced Security Requirements for Protecting Controlled Unclassified Information” are properly implemented in accordance with contractual requirements. The CMMC Program does not directly prohibit the use of TikTok on contractor devices. However, several of the NIST control requirements assessed via the CMMC Program ensure that contractors implement system policies that prevent personnel or automated processes from installing software such as TikTok, create and retain system auditing logs and records needed to monitor unauthorized activities, and ensure that such auditing logs are traceable to individual users to hold them accountable.

Mr. WITTMAN. The Cybersecurity and Infrastructure Security Agency (CISA) published in March the “Review of the Summer 2023 Microsoft Exchange Online Intrusion” that assessed the security failures of Microsoft which led to successful cyberattacks from Chinese and Russian hackers (ex: Fancy Bear and Midnight Blizzard). Additional cyber-attacks against Microsoft have been reported since the major incidents of 2023, leading CISA to issue an Emergency Directive 24–02. With regard to the Department’s use of Microsoft software, have you implemented any policies to mitigate exposure, through Microsoft capabilities, of the Department to TikTok or ByteDance applications? Furthermore, in the Midnight Blizzard attack, source code repositories and internal systems were compromised. Was the compromised code the same code of platforms upon which the Department relies? Does the Department rely on a single vendor for the majority of its Unclassified and Classified communications? And does DOD practice vendor diversity and “Defense in Depth” for these types of systems and software? Finally, it is my understanding the Army, and potentially other services and agencies, employ the full suite of Microsoft 365 services. Since the entire suite is closely integrated, to what extent has DOD been able to meet the CISA Emergency Directive to take immediate, remediating action for tokens, passwords, API keys, or other authentication credentials known or suspected to be compromised?

Ms. MANNING. The Department of Defense (DoD) utilizes multiple cybersecurity tools including Microsoft tools to mitigate exposure from applications such as TikTok. DoD applies network content filtering to all DoD networks to block access to the TikTok website. In addition, the DoD Chief Information Officer (CIO) memorandum on the “Use of Unclassified Mobile Applications in Department of Defense” dated October 6, 2023, outlines mitigations for mobile devices by segmenting DoD information from unmanaged and non-DoD applications such as TikTok or

ByteDance applications. While DoD employs Microsoft Windows and Office Suite for basic computing and communications, it also employs a wide variety of non-Microsoft technologies in support of its various missions. The DoD emphasizes vendor diversity per the requirements for competition set out in the Federal Acquisition Regulation (FAR). The Department is aware of the Midnight Blizzard compromise, which resulted in the exfiltration of email correspondence through a compromise of Microsoft corporate email accounts. These emails contain authentication details, which Midnight Blizzard is seeking to use to gain access to Microsoft systems. USCYBERCOM tasked all DoD components to investigate and mitigate the compromise. The tasking covers the Cybersecurity and Infrastructure Security Agency (CISA)'s Emergency Directive actions.

Mr. WITTMAN. The threat of Chinese cyber capabilities continues to be a persistent and penetrating issue for the Congress and U.S. Government in general. One of the vulnerabilities that Congress continues to address is TikTok. The Congress took action and banned TikTok on all government devices and devices that access government information. Given the young age of many service members, it is not presumptuous to assume that many of them have TikTok accounts and have downloaded the application on their personal devices. To protect the data of U.S. service members, personally identifiable information, and controlled and classified information, is the Department of Defense currently compliance with US Code S.1143—No TikTok on Government Devices Act? What is the Department doing to ensure that the TikTok ban is enforced, particularly on Government issues cell phones or any bring your own device solutions. Finally, how does the Department intend to enforce this Code with the contractors required and identified under CMMC guidance?

General HAUGH. Regarding the ban of TikTok on government devices, JFHQ-DODIN directed removal of TikTok “from all Government Furnished Equipment (GFE) and prohibit users from downloading or accessing the application in January 2023.” As a result, the Department is compliant and no government desktop or mobile device may access the TikTok application, as directed by U.S. Code S. 1143. JFHQ-DODIN leverages Security Information & Event Management (SIEM) tools to correlate and continually monitor the effectiveness of the ban across DoD issued devices. For off-DODIN contractors applying CMMC guidance, DOD CIO is best postured to provide a formal response, as they maintain the Department's CMMC website and are involved in the ongoing rule-making process that is part of the CMMC 2.0 phase-in period.

Mr. WITTMAN. The Cybersecurity and Infrastructure Security Agency (CISA) published in March the “Review of the Summer 2023 Microsoft Exchange Online Intrusion” that assessed the security failures of Microsoft which led to successful cyberattacks from Chinese and Russian hackers (ex: Fancy Bear and Midnight Blizzard). Additional cyber-attacks against Microsoft have been reported since the major incidents of 2023, leading CISA to issue an Emergency Directive 24-02. With regard to the Department's use of Microsoft software, have you implemented any policies to mitigate exposure, through Microsoft capabilities, of the Department to

TikTok or ByteDance applications? Furthermore, in the Midnight Blizzard attack, source code repositories and internal systems were compromised. Was the compromised code the same code of platforms upon which the Department relies? Does the Department rely on a single vendor for the majority of its Unclassified and Classified communications? And does DOD practice vendor diversity and “Defense in Depth” for these types of systems and software? Finally, it is my understanding the Army, and potentially other services and agencies, employ the full suite of Microsoft 365 services. Since the entire suite is closely integrated, to what extent has DOD been able to meet the CISA Emergency Directive to take immediate, remediating action for tokens, passwords, API keys, or other authentication credentials known or suspected to be compromised?

General HAUGH. While the Department of Defense (DoD) does not fall within the purview of the Cybersecurity and Infrastructure Security Agency’s (CISA) authorities, we remain in close coordination with CISA as it issues guidance to all federal Agencies under its authority. In concert with the DoD CIO and the National Manager for National Security Systems (NM-NSS), JFHQ-DODIN issues specific guidance and direction to the DoD for significant events such as the Midnight Blizzard compromise of Microsoft. Based on the information provided by Microsoft, there was no compromise of source code that would elevate risk to the department. In response to the events, JFHQ-DODIN released a Cyber Tasking Order directing hunt, clearing, and remediation actions based on potentially exposed DoD credentials immediately following the notification of the Microsoft Corporate network compromise. JFHQ-DODIN has released several orders over the last six months in coordination with DoD CIO to enhance data security measures, visibility, and detection across the M365 environment. As a result, the orders align the Department with the directed Zero Trust Framework. Additionally, the DODIN security concept is built around a Defense in Depth posture which uses various vendors overlaying several tiers of security tools/capabilities.

