

[H.A.S.C. No. 117-78]

**OPERATIONS IN CYBERSPACE AND
BUILDING CYBER CAPABILITIES ACROSS
THE DEPARTMENT OF DEFENSE**

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBER, INNOVATIVE
TECHNOLOGIES, AND INFORMATION SYSTEMS

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

HEARING HELD

APRIL 5, 2022



U.S. GOVERNMENT PUBLISHING OFFICE

48-633

WASHINGTON : 2023

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES,
AND INFORMATION SYSTEMS

JAMES R. LANGEVIN, Rhode Island, *Chairman*

RICK LARSEN, Washington	JIM BANKS, Indiana
SETH MOULTON, Massachusetts	ELISE M. STEFANIK, New York
RO KHANNA, California	MO BROOKS, Alabama
WILLIAM R. KEATING, Massachusetts	MATT GAETZ, Florida
ANDY KIM, New Jersey	MIKE JOHNSON, Louisiana
CHRISSY HOULAHAN, Pennsylvania, <i>Vice</i>	STEPHANIE I. BICE, Oklahoma
<i>Chair</i>	C. SCOTT FRANKLIN, Florida
JASON CROW, Colorado	BLAKE D. MOORE, Utah
ELISSA SLOTKIN, Michigan	PAT FALLON, Texas
VERONICA ESCOBAR, Texas	
JOSEPH D. MORELLE, New York	

JOSH STIEFEL, *Professional Staff Member*

SARAH MOXLEY, *Professional Staff Member*

PAYSON RUHL, *Clerk*

CONTENTS

	Page
STATEMENTS PRESENTED BY MEMBERS OF CONGRESS	
Langevin, Hon. James R., a Representative from Rhode Island, Chairman, Subcommittee on Cyber, Innovative Technologies, and Information Sys- tems	1
WITNESSES	
Nakasone, GEN Paul M., USA, Commander, U.S. Cyber Command and Direc- tor, National Security Agency	5
Plumb, Hon. John F., Incoming Principal Cyber Advisor to the Secretary of Defense, U.S. Department of Defense	4
APPENDIX	
PREPARED STATEMENTS:	
Banks, Hon. Jim, a Representative from Indiana, Ranking Member, Sub- committee on Cyber, Innovative Technologies, and Information Sys- tems	32
Langevin, Hon. James R.	29
Nakasone, GEN Paul M.	43
Plumb, Hon. John F.	34
DOCUMENTS SUBMITTED FOR THE RECORD:	
[There were no Documents submitted.]	
WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING:	
Mr. Moore	53
Mr. Moulton	53
QUESTIONS SUBMITTED BY MEMBERS POST HEARING:	
[There were no Questions submitted post hearing.]	

OPERATIONS IN CYBERSPACE AND BUILDING CYBER CAPABILITIES ACROSS THE DEPARTMENT OF DEFENSE

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON CYBER, INNOVATIVE
TECHNOLOGIES, AND INFORMATION SYSTEMS,
Washington, DC, Tuesday, April 5, 2022.

The subcommittee met, pursuant to call, at 4:21 p.m., in room 2118, Rayburn House Office Building, Hon. James Langevin (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, CHAIRMAN, SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

Mr. LANGEVIN. The subcommittee will come to order. Well, I—we got started later than I had anticipated, than we all had anticipated, due to votes.

But I want to begin by welcoming everyone to today's hearing, "Operations in Cyberspace and Building Cyber Capabilities Across the Department of Defense," and I'd like to begin, of course, by welcoming our witnesses.

Let me start welcoming, first, General Paul Nakasone, the Commander of U.S. Cyber Command and the Director of the National Security Agency, and Dr. John Plumb, who was recently confirmed as the Assistant Secretary of Defense for Space Policy and who serves concurrently as the Principal Cyber Advisor to the Secretary of Defense.

Welcome to you both.

Dr. Plumb appeared in front of the Intelligence and Special Operations Subcommittee on Friday. So this is only his second appearance as a witness for the House Armed Services Committee and the first on matters related to cyber issues.

John, I understand that you're a proud Notre Dame alum. I know that our Ranking Member Banks is extremely happy to hear this and I promise not to hold it against you, and look forward to your testimony in just a few minutes.

By the way, it would be appropriate for me now—right now, Ranking Member Banks is in the middle of markup on the—in the Labor Committee and so, therefore, I ask unanimous consent for Ranking Member Banks to deliver his opening statement later in the hearing when he arrives.

Without objection.

So, General Nakasone, it's always great to see you as well. I have valued our relationship over many years now. And I certainly admire your dedication to both your mission and your people.

We warmly welcome both of you to today's proceedings and look forward to working together and I look forward to your testimony, of course.

As I'm sure you've heard by now, and for the record, I do plan on not seeking reelection at the end of the 117th Congress. And after nearly 22 years in Congress, I'm ready to chart a new course, and I've cherished my time serving the people of Rhode Island's Second Congressional District and the men and women in uniform.

And over the course of my tenure, I've seen cybersecurity and cyber issues move from the periphery to the center of national security, and I'd like to think and I hope that I've played some small role in focusing the Congress on these vital matters.

So, out of curiosity, I looked back at prior years' National Defense Authorization Act. In 2001, my first year in Congress, the NDAA didn't even mention the word cyber or internet, not even once, as a matter of fact, and there certainly wasn't a combatant command dedicated to cyberspace operations at that time.

Today, cyber is part of nearly every issue that we deal with in national security. For Congress, not only does the word cyber appear much more than once but last year was the second consecutive year where the NDAA contains an entire chapter or title devoted to cyberspace-related matters.

For the Department, Cyber Command has not only been in existence as a unifying combatant command for nearly 4 years but is conducting operations day to day in and out—day in and day out in defense of our national security.

In the 3 years that I've had—I've served as chairman of the subcommittee, we have had more than 220 separate pieces of legislation across 3 NDAAs enacted into law.

This subcommittee, along with our colleagues from the Senate, have tackled, among many other things, cybersecurity of weapons systems; cyber warfare personnel pay parity; cyber targeting; support to the private sector and critical infrastructure; capabilities to defeat ransomware; budgetary authorities; cyber requirements for defense contractors; and of the most significance to me, the creation of the National Cyber Director role in the Executive Office of the President.

We no longer have to debate whether we will fight wars in cyberspace, and to some it may seem crazy that we ever had to have that discussion in the first place.

Cyberspace is recognized—is a recognized domain of warfare and for better or for worse our service members and civilians are engaged with our adversaries on a daily basis. The Department of Defense and military services have also undergone a similar transformation.

We have a dedicated combatant command for cyberspace operations. We have soldiers, sailors, airmen, and Marines, guardians and coastguardsmen defending our Nation in cyberspace, and we have witnessed the incredible outcomes for our national defense that we can create through cyber means.

And yet, for all the progress that we have made on this front, there can be a sense of déjà vu in the issues that we have—we still have to address.

On workforce matters, for instance, the points that we can and should make today are unnervingly similar to what was said at hearings 10, 15, and even 20 years ago, statements such as we struggle in competing with the private sector for talent, or there remains a critical shortfall in our cyber talent.

Since 2010, this body has legislated on cyber and STEM [science, technology, engineering, and mathematics] workforce issues through 55 provisions and sometimes we seem no closer than we were before. We continue to struggle in elevating considerations for cyber domain to a level commensurate with how we treat our land, air, sea, and now space domains.

And I've been in Congress long enough to know that progress with any important issue is always incremental. However, incremental does not have to be synonymous with glacial.

So the responsibility of legislators is tremendous, and we wield the tools at our disposal as carefully as possible. When an issue requires attention, we are judicious in how we direct the Department to respond.

Directive actions are powerful but resorting to these too frequently lessens their effect. That's why we often direct other actions such as reports, briefings, quarterly updates, implementation plans, designation of senior officials, and many, many others.

We use these to make clear the view of Congress. Though we use these tools because they're often successful in accomplishing the desired end state, it is not an exaggeration to say that we have tried to use these alternatives hundreds of times in the cyber context.

However, at a certain point, when we are discussing the same issues as our predecessors' predecessors, we have to ask ourselves can we continue trying—can we continue trying the same types of approaches that don't result in change.

So if we are repeating the same frustration on an annual basis about cybersecurity and the defense industrial base or the readiness of our cyber forces or the way in which the Department manages cyber issues, then at some point we must acknowledge a lack of preparedness to address these critical challenges.

Congress has great obligation to our national security. During my final year in these halls, I'm not interested in allowing my successor to inherit the same challenges that plague us today.

I look forward to being bold, to pushing for overdue changes, and to working collaboratively with our members and our witnesses.

So with that, I again want to thank our witnesses for appearing before us today. As a reminder, after this open session we will move to Rayburn 2212 for a closed member-only session.

As mentioned, we'll have unanimous consent request for Ranking Member Banks at this time we'll wait to—for him to arrive or we'll have his records—remarks inserted into the record.

So with that, I want to, again, thank our witnesses for appearing before us today and with that, as always, it's great to work with my colleagues on both sides of the aisle on these important issues and I will stop there.

And with that, I'd like to turn now to Dr. Plumb and General Nakasone for 5 minutes each to—for your remarks.

Dr. Plumb, please proceed.

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

STATEMENT OF HON. JOHN F. PLUMB, INCOMING PRINCIPAL CYBER ADVISOR TO THE SECRETARY OF DEFENSE, U.S. DEPARTMENT OF DEFENSE

Dr. PLUMB. Thank you very much, Chairman.

Thanks, Chairman Langevin, thanks, Ranking Member Banks and members of the subcommittee. I'm pleased to join General Nakasone, Commander of U.S. Cyber Command, to report on the progress the Department of Defense is making in achieving our objectives in cyberspace.

As Secretary Austin has made clear, China is the pacing challenge for the Department and that includes cyberspace. China believes that achieving information dominance in cyberspace will enable it to seize and maintain the strategic initiative in a crisis or conflict.

China's malicious ongoing cyber campaigns include exfiltrating sensitive info from U.S. public and private sector institutions and stealing U.S. intellectual property and research from the defense industrial base.

And while China may be the Department's pacing challenge, Russia is the near-term threat today. On March 21st, President Biden warned that Russia could conduct malicious cyber activity against the United States, including as a response to the unprecedented economic costs we have imposed on Russia alongside our allies and partners.

The President stated this warning is based on evolving intelligence that the Russian government is exploring options for potential cyberattacks.

And, of course, it's not just Russia and China. Iran and North Korea are threat actors of concern and ransomware criminals remain a persistent threat.

The Department recognizes the need to prioritize missions to disrupt threats overseas at their source in and through cyberspace. In a domain subject to constant change, our success in this mission demands the ability to conduct timely offensive cyber operations when the threats meet the threshold for action as established in policy.

The existing national policy framework, NSPM-13 [National Security Presidential Memorandum], enables the Department's offensive cyber operations and it has made important and positive contributions to the Department's ability to engage the threat.

The Department will continue to advance and modernize how we operate in cyberspace to engage cyber threats effectively and in a well-coordinated manner. The Department's superiority in cyber domain also depends on maintaining an ability to move quickly in a cohesive manner with key partners.

The close collaboration between the National Security Agency and U.S. Cyber Command, which is strengthened by the so-called dual-hat arrangement, has been a significant enabler of that suc-

cess. The DOD [Department of Defense] is currently conducting its 2022 Cyber Posture Review, which is an assessment of the Department's organizations, plans, programs, and policies germane to cyber operations.

Once complete, the Cyber Posture Review will inform the Department's 2022 cyber strategy. That strategy will provide guidance to the Department as to how its cyber combat power should be used to implement the National Defense Strategy and how in particular cyber operations will advance integrated deterrence.

The strategy will also identify potential solutions and paths forward for addressing any gaps identified in the posture review.

In the past year, we have seen cyber actors conduct malicious cyber activities at an unprecedented scale. Prominent examples include the Russian-led exploitation of the SolarWinds software, the Microsoft Exchange Server vulnerability exploited by the Chinese group Hafnium, and the Colonial Pipeline ransomware operation.

But the past year has also demonstrated that the Department, the U.S. Government, and our private sector partners can find creative ways to mitigate and combat these cyber threats. And today, today, the U.S. Government and the private sector are collaborating in unprecedented ways to prepare for potential Russian cyberattacks against the homeland.

DOD will continue to work closely with this committee as we seek to strengthen both our defensive and offensive cyber capabilities and mature our cyber forces. Our ability to successfully operate in cyberspace is essential to U.S. national security.

Thank you again for holding this timely hearing. I look forward to your questions.

[The prepared statement of Dr. Plumb can be found in the Appendix on page 34.]

Mr. LANGEVIN. Thank you, Dr. Plumb.

General Nakasone, you're recognized for 5 minutes.

**STATEMENT OF GEN PAUL M. NAKASONE, USA, COMMANDER,
U.S. CYBER COMMAND AND DIRECTOR, NATIONAL SECURITY
AGENCY**

General NAKASONE. Chairman Langevin, Ranking Member Banks, and distinguished members of the committee, I'm honored to testify beside Assistant Secretary Plumb.

I'm joined today by Command Sergeant Major Sheryl Lyon, the U.S. Cyber Command and NSA [National Security Agency] senior enlisted leader. We are honored to represent the military and civilian members of U.S. Cyber Command.

Command Sergeant Major Lyon and I want to recognize you, Chairman, for your 22 years of service to our Nation. Thank you for your advocacy, your passion, your commitment to not only U.S. Cyber Command and the National Security Agency, but most of all, our Nation.

Defending the Nation is at the heart of U.S. Cyber Command's mission. The command has been integral to the Nation's response to the current Russia-Ukraine crisis.

We have provided intelligence on the growing threat; helped to warn government and industry to tighten security within critical infrastructure sectors; enhanced resilience on the DOD Information

Network; accelerated efforts against criminal cyber enterprises; and together with interagency and allied partners, planned for a range of contingencies.

Coordinating with the Ukrainians in an effort to help them harden their networks, U.S. Cyber Command deployed a hunt forward team who sat side by side with our partners to gain critical insights that have increased homeland defense for both the United States and Ukraine.

U.S. Cyber Command views 2022 as a year of significant opportunity for building our capabilities as we pursue five priorities: readiness; operations in defense of the Nation; integrated deterrence; recruitment, retention, and training of the force; and the joint cyber warfighting architecture and enhanced budget control.

My goal is a command that remains world class, ready, and capable of providing options and conducting operations in defense of the Nation with wider partnerships and exceptional talent.

These elements will be essential to national security, as our Nation faces an array of adversaries who are expanding in scope, scale, and sophistication. Cybersecurity is national security.

Speed, agility, and unity of effort brought about by the connected relationship between U.S. Cyber Command and the National Security Agency is the ingredient that protects the United States against our enemies.

The men and women of United States Cyber Command are grateful for the support this committee and Congress has given to our command. I look forward to your questions.

[The prepared statement of General Nakasone can be found in the Appendix on page 43.]

Mr. LANGEVIN. Thank you, General Nakasone. I thank the witnesses for the testimony. We'll now move to questions.

Let me start. This is for both of our witnesses, and just for the record and to clarify. So, a media report recently claimed that the interagency is considering changes to the National Security Presidential Memorandum 13, or NSPM-13.

So this is an executive branch policy that governs a subset of cyberspace operations conducted by departments and agencies to include the Department of Defense. So NSPM-13 as a policy instrument, I believe, has improved the Nation's ability to conduct operations in cyberspace.

However, it's always important that we do our due diligence regarding oversight.

Dr. Plumb and General Nakasone, could you each speak to NSPM-13—how it's been employed to date, and if you're anticipating any changes? I'll start with that.

Dr. PLUMB. Thank you, Mr. Chairman. I'll take that first and then pass it to General Nakasone.

But I guess—let me just answer the top piece of this question was, one, NSPM-13 has been valuable. It clearly has improved the ability to conduct cyber operations, and, you know, thank you to this committee and the general's good work and all those that have got us this far.

I also would just say I don't think it's unreasonable or new for a new administration to review existing Presidential directives and so that is kind of a standard piece, and I think that that is a rea-

sonable expectation and it is correct that these conversations are ongoing.

And I think our goal, at least my goal and I know I share it with the general, is to make sure that we preserve our ability to move at speed.

Mr. LANGEVIN. Yeah. I agree with you that a review is appropriate always for a new administration. But to date, are you expecting any significant changes in NSPM-13 right now?

Dr. PLUMB. So I am—I don't want to box anybody in on that. I'm not expecting any changes that would make things anything except better. But maybe we could pass it to the general and he can give you his military insight on that if that's all right.

Mr. LANGEVIN. Okay. Thank you.

General.

General NAKASONE. Chairman, in light of NSPM-13 in 2018, I think it was one of two major advances in terms of authorities and policies that provided us the impetus to take effective action in cyberspace.

The other one, as you recall, was declaring cyber as a traditional military activity, which came in the fiscal year 2019 NDAA. Both of those have been very helpful to us.

In terms of changes, obviously that's a policy discussion that's ongoing now. I'm sure those discussions will continue. I know that my discussions with the Under Secretaries and also the Secretaries—I've made my military knowledge known in terms of what NSPM-13 has meant to us.

Mr. LANGEVIN. Okay. Thank you. Thank you, General.

This is obviously something we'll want to continue to follow up and I get—you know, having read through the NSPM-13 document when eventually it was forwarded to the Congress for review that, you know, I support its premise and the document as it's written and, hopefully, any changes made would make it—would make it better, but, hopefully, not a sharp deviation from it.

General, let me just turn to you. In past appearances in front of the subcommittee, we have discussed the cyber mission force [CMF] and its size.

With the benefit of time, can you speak to USCYBERCOM's [U.S. Cyber Command's] plan to—for planned growth in the CMF? Additionally, can you speak to the differences you've witnessed, say, from last year to this year and, you know, the work that still continues to evolve as the force grows and matures?

General NAKASONE. Chairman, as we originally built the force in the Department, 133 teams that were dedicated to our cyber mission force. The previous Secretary of Defense has approved a 14-team growth in the FYDP [Future Years Defense Program]. So we're going to grow five more teams this year.

The question I often get asked is, is this enough? What's the number of teams that you need? And this is a study that's ongoing right now within the Department to really determine what is the final number of teams that we need for the future.

My sense is we are learning a tremendous amount of our operations right now in support of crisis in the Ukraine that will likely inform this.

We're a different force today than we were even 4 years ago when I took over, and so my sense is that while 14 teams is likely the start, I would not be surprised if the Department comes to a determination that more are necessary.

Mr. LANGEVIN. Thank you, General, and, you know, based on your time in command at Fort Meade, can you speak to the comparison of authorities between CYBERCOM and SOCOM [U.S. Special Operations Command]?

And, more specifically, are there specific authorities that SOCOM has today which are applicable and would be useful for you in your operation?

General NAKASONE. Chairman, as you're aware, one of the things we did when we designed U.S. Cyber Command well over a decade ago was to look at Special Operations Command as perhaps an exemplar of where we needed to go.

What you speak of is what we term service-like authorities—what are the service-like authorities that we should emulate that U.S. Special Operations Command has today?

So right now, the authorities they have with regards to training; the authorities they have with regards to joint force provider and overseeing the provision of teams; and then the last piece is acquisition.

All of those, Chairman, are areas that we think we need to be able to emulate more closely to have that service-like appearance for what we do.

This is important for us because, as you are well aware, this comes down, at the end of the day, to the personnel, the personnel that train, the personnel that are trained on teams, and the effectiveness of these teams. All of those areas are areas that we're focusing on as we move forward.

Mr. LANGEVIN. Thank you. Okay. I'm going to stop there. If we go to second round or we have the opportunity to go to the classified session for more detailed answers, but with that, I'm going to yield right now to Mr. Franklin.

Mr. FRANKLIN. Thank you, Mr. Chairman. You asked some of my questions about the growth in the teams. That's encouraging, General, to hear that there are 14 more slated. CYBERCOM has shown a great deal of commitment to building both capability and capacity with the cyber mission force, reaching full operational capability ahead of schedule.

We see further maturing. I do know in the State of Florida we have got training units at Corry Station and at Hurlburt Field, both successful operations.

How are we learning from these institutions to help develop cyber-related curricula and building sustainable readiness across the force?

General NAKASONE. So one of the most important ways that we're learning is really twofold, Congressman. One is that our force is learning every single day in the operations that we're conducting in cyberspace. This is a force that's engaged against a variety of adversaries every single day of the year.

And so the important piece is how do we take those lessons learned every day and bring them back to a place like Corry Sta-

tion or Pensacola, and that's one of the things that we certainly have done.

But the second piece is, I think, also important. That is, the people that have led our teams, the people that have operated on our teams, the people that have been in hunt forward missions in different countries, how do we get them back into the schoolhouse, that they are the principal trainers of our young people that come forward?

Mr. FRANKLIN. General, the fiscal year 2023 budget contains \$11.2 billion for cyberspace activities and that's a 7.6 percent increase year over year, which sounds very strong, and a few months ago, I would have thought that would be the case.

But considering we're now at 7.8 percent inflation, it's actually a net decrease. I realize there's a lag time between when you all are putting budgets together and when they finally get out there. But is your determination that the cyber threat to the country is stagnant or decreasing?

General NAKASONE. That is not my determination in terms of my view of the future. I think it's increasing in terms of what our adversaries present to us as a nation.

Mr. FRANKLIN. So I know we had a long hearing earlier today about the fiscal year 2023 budget, but this is a budget that fails to keep pace with inflation.

Are you are you confident that you will be able to make do and, like good soldiers, salute and carry out the plan of the day? But is this budget adequate or do you—are you—would you be asking us to plus that up?

General NAKASONE. So, Congressman, the amount that's been funded to us today is what we need to start with. But we have also identified unfunded priorities and we'll provide that to the committee as directed by the NDAA.

Mr. FRANKLIN. Okay. Thank you.

Dr. Plumb, what is your assessment of our ability to deter cyberspace attacks on the U.S. Government and critical infrastructure, in general?

Dr. PLUMB. Thanks, Congressman.

Defending the homeland, deterring cyberattacks of at least, I guess I would say, a strategic nature, absolutely essential.

I think—I guess what I would offer is I don't think cyber deterrence is a piece unto itself. So I think deterrence comes—you know, we have been using this term integrated deterrence. I'm sure you've—you're well aware of it. I know everyone here is.

But you don't deter cyber just with cyber alone. You deter with all instruments of national power. And I think, at the moment, the President has used the megaphone of the United States of America to warn the Russians not to attack critical infrastructure.

At the same time, through Cyber Command and through our Department of Homeland Security partners, we have been working with private sector and the defense industrial [inaudible] to make sure that people's shields are up, that they're ready, that they're being alerted to threats.

So I think part of that is the defense piece. Part of that is warning of retaliation. And I think—I actually think that is, at the moment, holding.

Mr. FRANKLIN. Okay. Are there additional tools or resources or authorities that would be helpful to help bolster our ability to deter these cyber—or cyberspace attacks against the country?

Dr. PLUMB. I think on the specific question of tools, I would ask the general to answer that. I don't know if that's answerable in this session. I don't have any—I believe the authorities are in place. I believe the authorities are in place at this time.

Mr. FRANKLIN. General, unclass [unclassified], would that—anything you would want to offer in this setting?

General NAKASONE. So I have the authorities that I need right now, Congressman, to accomplish my mission. Obviously, we look at a series of partnerships, and no one department or agency can do it all in cyberspace.

So what we are very focused on is how do we develop partnerships with CISA [Cybersecurity and Infrastructure Security Agency] and with FBI [Federal Bureau of Investigation] and with foreign partners and, most importantly, the private sector to ensure that we all have a common vision and a common vigilance.

Mr. FRANKLIN. Thank you, gentlemen.

I yield back, Mr. Chairman.

Mr. LANGEVIN. Thank you, Mr. Franklin.

Mr. Moulton is now recognized.

Mr. MOULTON. Great. Thank you, Mr. Chairman.

And, gentlemen, thank you very much for being here, for your ongoing work.

This morning, Chairman Milley listed four primary elements of national power, one of which is informational, and it sounds quite important in that context. And yet, information operations is buried in the organizational structure of DOD and many experts feel that our capabilities have been significantly degraded over the past decade, this as we watch the value of information warfare play out on the ground in Ukraine.

Do you believe that information operations is a warfighting function that fundamentally should be in Cyber Command or should it be elsewhere in DOD?

General Nakasone, if you could take a crack at that first, please.

General NAKASONE. All right.

So, Congressman, it already is in Cyber Command. I think what I would say is that what have we learned about information. Information always has to be paired with our cyber operations to make them even more effective.

Information is only as effective as it is accurate, timely, and relevant, and that ability for us to do that needs to pair with the type of work we're doing either defensively or offensively.

We have come a long way since 2018 in working the information operations, but we still have a long ways to go.

Mr. MOULTON. Thank you, General. I mean, my frustration is that, to me, cyber is one of many, many delivery methods for information and it doesn't make sense to me that it's buried in a command that's just one of the delivery methods rather than on a more strategic level.

But I understand the fact that you own it and you're going to defend it.

Mr. Plumb, what's your view on this? Do we have the right organizational structure for information operations, or should we be looking at reorganizing within DOD?

Dr. PLUMB. So, Congressman, thanks for the question and, obviously, information warfare, if you wish, has been really essential, really, over the last month or two here with the Russia-Ukraine conflict.

I guess I would say, on one level, we are conducting information operations to a strategic level with the President and the White House making announcements.

Mr. MOULTON. I understand that, Mr. Plumb. But I'm asking about the organizational structure within DOD.

Dr. PLUMB. So on the organizational structure, I'm going to ask you if I can take that for a lookup.

[The information referred to can be found in the Appendix on page 53.]

Mr. MOULTON. Okay.

Dr. PLUMB. I'll say I don't have anything immediate, but I don't want to leave something—

Mr. MOULTON. That's fine. If you can take that for the record, that would be great.

General, you mentioned to me earlier that the USMC—the Marine Corps—has done a great job of retaining its cyber workforce and the Marines are planning further changes and reforms to their personnel policies, including directly commissioning cyber operators and other specialties into higher ranks, as was commonly done with various specialties during World War II.

Do you believe these additional changes are warranted and will help further retain the workforce?

General NAKASONE. I do, and I see it already. I've seen it in my own service in terms of, first of all, building a branch, then taking a look at different initiatives in terms of what they do.

What the Marines have really done very efficiently that I applaud is the fact that they've lengthened their tours in terms of how long they stay with us.

Most young men and women that come into the Marine Corps that want to be cyber warriors want to do cyber, and so being able to do that for 6-plus years at one location has been very, very attractive to them and we see that in the payoff with regard to the retention numbers.

Mr. MOULTON. General, you described the mission of CYBERCOM in your opening statement as defense—defense of the Nation. What role do you see for offense and deterrence?

I know we talk about integrated deterrence but when we really talk about having an effective deterrent it means having an effective offense. So what—how do you characterize the role of offense to the American people?

General NAKASONE. So, Congressman, when I speak of defense of the Nation, that is a full spectrum defense to include offensive operations. You know, the best defense a lot of times is a good offense.

The way that we have done this at U.S. Cyber Command is the idea of persistent engagement—how do we maintain both the ability to share information and act against our adversaries.

We don't want those adversaries to continue to have free rein in terms of what they do in cyberspace. So how do we ensure that when they steal our intellectual property or when they steal our identities or when they try to interfere within our elections, we take them on, and that's what we have done since 2018.

Mr. MOULTON. But if I can press you a bit on this, I mean, it's common knowledge, without going into anything classified, that the Chinese are stealing our intellectual property every single day.

They're sometimes effective at getting it from DOD but they're effective all the time at getting it from the private sector. Do you think we should have a more aggressive deterrence with China?

General NAKASONE. So I think in terms of the way that we look at our adversaries, such as China, is this needs to be not only persistent engagement but how do we look at the authorities in terms of what's being done in the United States and what is, you know, available for the Chinese to operate so freely within our Nation?

So I think that that has to be a more—a greater perspective on how we're going to do this in the future.

Mr. MOULTON. Thank you, Mr. Chairman. I yield back.

Mr. MOORE. Thank you, Chair. Thank you both for being here. General Nakasone, it's good to see you again. Appreciate the opportunity to talk about these growing and ever important issues now.

Thinking about our adversaries, one thing that's very concerning is the cybersecurity of the commercial and government entities of many of our adversaries, they're in lockstep, right.

They're operating, you know, I would almost say not even necessarily in a commercial way. That may be even just a front, right. Like, they're really operating in lockstep where, you know, you contrast that with American cyber mentality kind of an every man for himself. It's a way to categorize it. I know there's nuance to that.

But I am concerned that we're setting ourselves up to lose that competitive edge. Without stronger U.S. cyber public-private partnerships with regulatory and acquisition authority, America's technological—may become an exploitable vulnerability.

A question—I'm interested in this—I'm interested in improving our cutting-edge innovation efficiently and transitioning those programs of record.

Few things disincentivize information—innovation more than technologies and products languishing in the proverbial sort of, let's say, valley of death in the acquisition process.

I believe we can accelerate the adoption of emerging technology and strengthen our defense innovation base by empowering unit commanders who are responsible for mission outcomes impacted by rapidly changing technologies such as AI [artificial intelligence], SAS [statistical analysis software], quantum computing.

Would you support an innovation fund available at the installation or the installation command level to provide the experts on the ground the flexibility to pursue, develop, and integrate new emerging technologies?

General NAKASONE. So, Congressman, I would offer that we have some of that today and I think, you know, working with, you know, DIU—you know, Defense Innovation Unit—being able to work at a facility like we have at USCYBERCOM called DreamPort where,

you know, private companies are able to understand what our needs are and then rapidly adopt it.

It isn't necessarily a means of not having enough money. It's the fact that what we are doing is trying to cut down the barriers to make sure that the private sector understands our needs and rapidly they're being able to meet those needs. We have had some success there.

We need more. And I think that's, you know, more empowered by this idea of being able to have a number of different touchpoints such as Defense Innovation Unit and DreamPort available to our folks readily.

Mr. MOORE. So DIU's—we have interacted with them from our team, have had very positive interactions and I really appreciate the shift that we're really trying to make here, taking commercial products—taking what's commercially available and making it very relevant and useful in our DOD. So it's a good—please.

General NAKASONE. So, if I might follow up on it. So meet very frequently with Mike Brown, you know, who's the leader of DIU. What has been most effective for us is for them to understand these are the challenges that we would like to have you go and see what the private sector may have. And so they've done that readily and I think we're starting to see some of the benefits of that.

Mr. MOORE. With it not being as much, as you say, the funding issue, more of a regulatory and, you know, that kind of conversation, we're welcome to that. I think that you would get a lot of support from this committee on helping navigate that.

Also, General, my bipartisan bill, the Better Cyber Crimes Metric Act, passed the House last week. It will improve the way Federal Government tracks, measures, and analyzes cyber crime.

However, I'm concerned we still do not have enough to incentivize private businesses and industry to share with the government when cyberattacks occur.

While you and I know—we know this not to be true, many business owners have been told that they have low confidence the government will do anything if hacks are reported. Do you have any recommendations on how to increase the willingness of private companies to share information when these attacks do take place?

General NAKASONE. Congressman, if I might take that for the record, just because I'd like to think about that a bit more. I know it's a very difficult question and I want to make sure I give a full-some answer.

[The information referred to can be found in the Appendix on page 53.]

Mr. MOORE. Okay. Excellent. That's—I've interacted with our Utah network quite a bit. We have a really awesome group of cyber professionals, startups, that's going on, that's being taught at our universities.

It's a burgeoning area and we're really excited about it, and they're really engaged and they want to help. They want to be involved in the work they're doing for the mission and for the pride of their country. So I appreciate any response that you have with that.

We have historically led the world in developing cybersecurity initiatives and standards, and as I've talked to those experts,

they're waiting to implement new forms of security approved or recommended by key government entities to ensure that businesses are not using technologies that may not receive future approval for government use.

This has undoubtedly slowed the adoption of new cybersecurity technologies. What is CYBERCOM doing to help inform and assist private partners with legacy security systems strained by the rapid proliferation of new computing form factors?

General NAKASONE. So, Congressman, our focus has been on the defense industrial base [DIB]. That's where the Secretary of Defense is a sector risk management authority. And so we have worked closely with both the National Security Agency and our private DIB partners to make sure that they have both an understanding of the threat and understanding of ways that they can rapidly get after that threat.

Mr. MOORE. Thank you. My time's up.

Mr. LANGEVIN. Thank you, Mr. Moore.

Ms. Escobar is recognized for 5 minutes.

Ms. ESCOBAR. Thank you so much, Chairman, for holding this hearing. It's a great opportunity for the committee to examine the functions of CYBERCOM and inform the American public of the critical role it plays in our Nation's cyber strategy.

As more and more of our daily lives move onto the web, it's essential that our country have top-of-the line cybersecurity defenses. This is especially critical for me because I represent El Paso, Texas, a border region with over 800,000 people that is also home to one of the largest installations in the Department of Defense, Fort Bliss.

General Nakasone and Secretary Plumb, I'm going to ask both of you the same question. One of the recurring topics on border security over the last years—the last few years has been technology.

I'm a firm believer that appropriate technology can and should be used to perform certain security functions and that deploying more strategic technology at our land ports, in particular—our land ports of entry—can decrease wait times for both cars and pedestrians, moving trade and commuters more quickly and more securely.

However, the use of this technology does raise certain questions, including how well fortified it is against potential adversarial cyberattacks.

General and Secretary Plumb, you mentioned working in an interagency manner with the Department of Homeland Security. Is there any interagency collaboration between CYBERCOM, the Department of Defense, and the Department of Homeland Security on the cybersecurity being provided for the ever-expanding technology being used at our borders?

General NAKASONE. Congressman, thank you very much for your question and your emphasis on cybersecurity.

While U.S. Cyber Command does not have that relationship, the National Security Agency, of which I head—does have that relationship with the Department of Homeland Security to provide that type of support with regards to cybersecurity. Now, that's something we do regularly with the Border Patrol based upon the request of the Department of Homeland Security.

And so this is something that is an ongoing mission for us at NSA and it's something that the DHS [Department of Homeland Security] and NSA regularly talk about.

Ms. ESCOBAR. Great. And, actually, Secretary Plumb—thank you so much, General—does the Department view the expansion of technology at our borders as another avenue that a foreign adversary may seek to exploit if the proper cybersecurity precautions are not taken?

Dr. PLUMB. Thank you, Congresswoman. I would say every technology has an avenue for exploitation that an adversary could use.

Ms. ESCOBAR. Thank you.

General, we had a discussion last year about CYBERCOM's efforts to recruit a diverse workforce. As I mentioned then, I represent the University of Texas at El Paso, which is a Hispanic-serving institution with a strong track record with the NSA as a National Center of Academic Excellence in cyber operations.

In your written testimony, you mentioned CYBERCOM's academic engagement network. I'd like to give you an opportunity to expand on the work you've been doing with that initiative and others to not just engage with academia but to recruit talent that comes from every corner of the country, including traditionally underrepresented populations.

General NAKASONE. Congresswoman, I welcome your invitation to do that. As you well know, we stood up the Academic Engagement Network at U.S. Cyber Command just this year and part of that is to be able to recruit a much broader demographic of our Nation. We need a force that's reflective of our Nation and this is one of the ways that we're doing it.

I must, in all transparency, tell you that our focus has been in San Antonio of late and so maybe we need to go a little bit further to the west in Texas to take a look at what El Paso has to offer there. But if you don't mind, let me take that up in the coming year.

Ms. ESCOBAR. I would invite you to do that and, in fact, would be happy to host you for a visit at the University of Texas at El Paso in El Paso, and then would love to follow up with you at some point in the near future about any lessons that you've learned since the start of the Academic Engagement Network, anything that you'd like to share with us so that we can continue to build on the work that you've begun.

Mr. Chairman, my time has just about expired. I yield back.

Mr. LANGEVIN. Thank you, Ms. Escobar.

Mr. Fallon is now recognized for 5 minutes.

[No response.]

Mr. LANGEVIN. Do we have Mr. Fallon?

Mr. FALLON. Yes. Yes, sir. Thank you. Thank you.

Mr. LANGEVIN. Very good. You're recognized for 5 minutes, Mr. Fallon.

Mr. FALLON. I was promoting you.

[Laughter.]

Mr. FALLON. Thank you. Listen, I think one of the mistakes that the public makes when it comes to cyber defense policy is the idea that this is somehow a new realm. However, you know, the threats in cyberspace aren't new and they've long since—we have long

since possessed both offensive and defensive capabilities, and competition in cyberspace, of course, is almost constant.

Even though this problem has been an issue for a long time, I have a substantial concern that the Department of Defense is still not properly positioned to address it in today's rapidly evolving landscape.

My concern is that there are too many—maybe too many chefs in the kitchen, if you will. I understand CYBERCOM is a joint force comprised of service cyber components from each of the branches.

And on top of that, you have Cyber National Mission Force and Joint Force Headquarters and DOD Information Network. I mean, already that becomes seven separate commands. Mix in CYBERCOM's commander's dual role as Director of the NSA and Chief of Central Security Service and you get another one.

Finally, throw in the rest of the intelligence community, the Department of Homeland Security, Department of Justice, et cetera, and I think you see where I'm going with this. So what do you get? A whole lot of bureaucracy and finger-pointing and not a highly adaptable organization ready and willing to fight and win.

Everybody wants to be in charge and everybody wants to, you know, maybe get the credit or pass on the blame if that's the case.

Dr. Plumb, can you honestly say that our cyber mission force is not hampered by this bureaucracy, and if you think there is a bureaucracy issue, what can we do to streamline it?

Dr. PLUMB. Thank you, Congressman. I agree with you that we need to make sure that bureaucracy doesn't get in the way of delivering military effects where needed.

I actually think that we are in pretty good shape at the moment. There's always room for improvement and always have to be—anyone that works in the Pentagon or, really, the government knows that you always have to be careful to guard your ability to not have more bureaucratic growth slow you.

I think the trend line, though, for cyber effects in particular has—is on—is going in the right direction. As we said at the beginning, sir, NSPM-13 has provided improvements in the ability to use cyber to advance the national interest and my goal in this role is to make sure that that trend line continues in a positive direction.

Mr. FALLON. And do you think there's—what things specifically—and you don't need to say it right now if—or if you want to get back to us—but how can we maximize efficiency? I just want to—I just want us to be thinking along those lines.

General, just for time's sake—General Nakasone, we have heard some complaints from within CYBERCOM that, you know, one day they work for one person and their priorities. Then the next day it changes. How do we create a unified vision and mission to set—to avoid subordinate commanders working on, you know, pet projects in silos, if you will?

General NAKASONE. So, Congressman, I'm not aware of that. I would tell you that there's one person in charge of U.S. Cyber Command and that person is me and we haven't—I have not seen that in terms of being able to develop options or being able to respond to crises for the Nation.

One of the opportunities that we have here is the fact that we have a very flat organization. While we may have a number of different headquarters, the teams all fall under the operational control of the commander.

And so while we have different missions that we support different commanders, there is no problem in terms of being able to develop the options and the requirements and, I would tell you, the effects for what our Nation needs.

Mr. FALLON. General, we recently created a new service in the Space Force. You know, cyberspace is a realm, of course, that touches everyone everywhere.

Do you believe there's any merit to creating another service designed to support all others, you know, like absent of territorial commands from subordinate commanders that can focus solely on cyberspace across DOD?

General NAKASONE. Congressman, I don't see this right now. One of the areas that I think has been very effective, as the chairman had indicated, we have service-like authorities to train the force, to be able to provision the force, to be able to do acquisition.

I would be very concerned on a new service in terms of what—you know, what you would call the bureaucracy that we'd be set up there. We're looking for, you know, our services that do a very, very good job of recruiting and training and then for us to be able to employ them rapidly.

Mr. FALLON. Okay. Thank you, Mr. Chairman. I yield back.

Mr. LANGEVIN. Thank you, Mr. Fallon.

And now Mr. Larsen is now recognized for 5 minutes.

Mr. LARSEN. Thank you, Mr. Chair. I appreciate that, and thanks for coming this afternoon.

General Nakasone, this is somewhat related to the question you just asked but I'm asking it in a different way to maybe sort of dig into a little bit about the construct of the CYBERCOM integrated planning elements and the joint cyber centers, if that's the most optimized mechanism for coordination between CYBERCOM and other COCOMs [combatant commands].

General NAKASONE. So I've seen it both ways, Congressman. I've lived long enough now to see both the joint cyber centers and now what we developed over the previous years, the integrated planning elements.

Let me tell you why I think the integrated planning elements are really what has been very effective for us. We have taken and designed an integrated element that goes to each of the combatant commands, the other 10 combatant commands, and it varies in size from 39 to 50 folks.

What that provides the commander are people that really understand cyberspace, that understand how we do our operations, how we do our planning, how we do our execution.

They're resident today with General Wolters at U.S. European Command. In fact, they are resident today to really understand and be able to provide General Wolters' staff the options that are necessary, both defensively and offensively, that are effective.

Why do I think this has been effective is because the feedback that I'm getting from the commanders is that they really value this type of integration.

Mr. LARSEN. So when they are with the COCOM, does COCOM then have an operational command of those folks, so they're setting the missions, whereas you've—perhaps you've done the training and equip part of the mission? Is that how to think about this?

General NAKASONE. They go embed themselves within different parts of the staff within the COCOM. That's designed by the combatant commander.

Mr. LARSEN. Uh-huh. Yeah. Well, maybe take a look at that.

But a little bit more on that point, though—thanks for bringing up EUCOM [U.S. European Command]—and again, I apologize. I was out. But there was an article last month, “Cyber troops stretched thin in Ukraine,” and I don't know how you can—if you can answer this or not, but how you see U.S. capabilities currently coordinating or integrating with allies and partners in any—in any current operations that are based in EUCOM.

General NAKASONE. So we can talk about this in more detail in the closed session. But what I would offer here is that one of the very big lessons that we have learned is the ability to deploy a number of different teams early on in a crisis to U.S. European Command, and then working with General Wolters and his staff, making sure that those experts, those teams, go to the places that are necessary.

And I can provide a little bit of thought in terms of where those teams have gone when we meet a little later on today.

Mr. LARSEN. Are there broader lessons to learn about what would—what would trigger the decision to send those teams? It seemed kind of—it seemed somewhat obvious in the current case, let's say, but there may be other cases in the future where it may not be as obvious that, oh, it's time to send teams. So what are you learning about looking into the future?

General NAKASONE. So what we have learned over nine different hunt forward operations in 2021 is the fact that consistent engagement with a series of partner nations is really valuable. We understand the networks. We understand the leadership. We understand what they care about most.

And so working with that, you know, in competition or crisis is much better than, you know, waiting until there's a conflict.

Mr. LARSEN. Right.

General NAKASONE. And so that's what we have learned.

Mr. LARSEN. Mm-hmm. And I'm sorry, Mr. Chair. Did folks ask questions about education requirements or anything else?

So yeah. So how are we doing with the pipeline of people that CYBERCOM can utilize in the future?

General NAKASONE. Broadly, I would say, Congressman, is our supply is not large enough in our Nation. And so as you well know, within the State of Washington with a number of different centers of academic excellence, we follow this up now at U.S. Cyber Command with the Academic Engagement Network to be able to build a resource for our Nation and that doesn't necessarily mean that they will come in as military civilian members of the Department of Defense, but the ability for them to have exposure and interest in what I think is, obviously, you know, a key competitive advantage for our Nation in the future.

Mr. LARSEN. All right. That's fine. Thank you. And I yield back.

Mr. LANGEVIN. Thank you, Mr. Larsen.

Mr. Johnson is recognized.

Mr. JOHNSON. Thank you, Mr. Chairman, and thank you, General, for your time today. In your role, you are responsible for the cyber operations that protect the sprawling .mil digital enterprise that our warfighter really depends upon, and over the last several years, progress has been made to implement an internet operations management program that looks at DOD's cyber infrastructure through the eyes of the adversary.

But despite some progress, this program has yet to be deployed across the entire DOD Information Network [DODIN], and recently enacted fiscal year 2022 DOD appropriations provide funds to do that.

So are you committed to pushing this critical endeavor across the finish line this year? Should we expect that?

General NAKASONE. I am committed, Congressman, and I would say, first of all, thank you for discussion on the DOD Information Network, a sprawling network in terms of, you know, what provides us support for our warfighting functions, our communications, and our capabilities.

What we have done with our joint force headquarters that's in charge of the DOD Information Network is look at all 45 stakeholders within this information network and then make sure that we're checking in terms of how they're conducting their operations.

This is part of the—you know, the foundational work that we need to have a much more secure and resilient DODIN.

Mr. JOHNSON. Very good.

And could you describe how CYBERCOM is integrating artificial intelligence and machine learning to automate defense of the DODIN and monitor it and identify cyber threats?

General NAKASONE. Congressman, we have worked a number of different experiments. I know of specifically an experiment that we worked at Army Cyber to look at artificial intelligence and machine learning to identify vulnerabilities within our network and then patch them automatically.

This is a really good example of taking, you know, what we would consider, you know, a vulnerability and not having to have a human in the loop but rapidly being able to address the vulnerability with a patch before anyone knows it.

This is the initial work that we have done. There's more work that needs to be done in AI. I'm a very, very strong supporter of the AI National Commission and where we can bring that to U.S. Cyber Command.

Mr. JOHNSON. And I know that some of this is sensitive and may be better in a classified setting, but I'm just wondering about what the most promising applications of AI and ML [machine learning] may be for the CYBERCOM enterprise.

General NAKASONE. There are many, Congressman, and I think that I will defer that to a different venue to, perhaps, have that discussion with you.

Mr. JOHNSON. Very good. Let me ask you about something else. I've got a couple minutes here. The late scholar Thomas Schelling described bargaining power is the power to hurt. Could you de-

scribe the utility of the defense forward concept compared to a more traditional deterrence by the punishment model?

General NAKASONE. So, as, you know, Secretary Plumb indicated, cyber deterrence is not nuclear deterrence and this is a much different, you know, means upon which we look at this domain.

And so what we have learned, I think, over the past several years is that we have to have an ability to really drive the cost up for our adversaries and there are a number of different ways that we can drive the cost up for our adversaries.

One is we can have much more resilient networks. Two, we can share information more broadly. Three, we can take on cyber adversaries that are attempting to attack our Nation. Those are all ways of doing it.

But it's a comprehensive approach. And the other piece that I would add is what we have learned from elections is that partners matter and partners like the FBI, partners like CISA, partners like academic institutions that have, you know, knowledge that they're tracking on adversaries that we may not even see.

And so I think, again, to the point of there's no one agency, no one department, that can do it all in cyberspace, but the most effective ones are the ones that partner and get it done together.

Mr. JOHNSON. Very good. Thank you again, General.

I yield back.

Mr. LANGEVIN. Thank you, Mr. Johnson.

Mrs. Bice is now recognized for 5 minutes.

Mrs. BICE. Thank you, Mr. Chairman, and General Nakasone, it's good to see you again.

The emergence of new technologies like artificial intelligence and quantum computing and the proliferation of cyber intrusion capabilities pose significant threats to our national security and to our service members.

One of my key concerns impacting the Nation's cyber posture is the workforce challenges that we face. As you are both well aware, it is critical that we get more trained cyber professionals into the door at U.S. Cyber Command.

With the tremendous competition in the private sector for cyber talent this is a huge challenge.

General Nakasone, can you briefly describe the U.S. Cyber Command's efforts to recruit and retain top talent in the face of stiff competition from the private sector?

General NAKASONE. Congresswoman, thank you very much, and it's good to see you again as well.

Let me begin, first of all, with the recruit piece. This is an area that I think our services who have a responsibility—Army, Navy, Air Force, Marines—to recruit talent have done exceptionally well.

We continue to recruit a population of young men and women that want to serve our Nation and they want to work in cyberspace, which is incredibly attractive to them.

The challenge is not necessarily the recruiting. The challenge isn't the training. The challenge, as you've indicated, is the retention and that's both for military and civilian.

Let me give you two ideas in terms—or several ideas that we have approached it. One is, certainly, targeted supplements to very, very high-end capabilities. So this is targeted local supplements

based upon people that are coders or people that have significant technical abilities, that pay them at 28 percent more than the going rate.

That's never going to, perhaps, compete with the private sector. But what it does do it does give us a leg up in being able to say what you do is valued and what you do is, obviously, renumeralated.

The other piece that I would say is a certain amount of dynamic of how we approach cyberspace and one of the things is, as the Congressman mentioned, you know, being able to do recruiting is, you know—from, you know, a population of civilians is, hey, come in and be a mid-grade officer. Or, as we take a look at our enlisted workforce and say, hey, why don't you go and spend 6 months in training with industry or going to get a graduate degree?

These are all areas that, perhaps, we haven't traditionally done within our services. But this is the dynamic nature that I think we have got to approach the problem here in cyberspace.

So as I've talked to the service chiefs, one of the areas that I've mentioned is this is a shared responsibility, shared in terms of what you have to do as leading your service but also shared in the idea we have a lot of different areas that we need to be able to make sure that we keep our best people.

Mrs. BICE. I love your thinking outside of the box approach to this—the problem because I think we have to figure out how do we keep and retain this crucial talent.

One other, maybe, thought here is how are you competing with DHS when it comes to pay for these individuals? It's my understanding that CISA folks are paying significantly or can pay significantly more than you're able to do. Is that something that Congress needs to look into?

General NAKASONE. So we're working with the Department right now in terms of, you know, how we have to look at that. That's not only as my role as Commander of U.S. Cyber Command. It's also my role as Director of NSA because we do see, you know, increased competition.

But again, you know, I think this is something that work closely with the Department, working, obviously, through Secretary Plumb as well as the Principal Cyber Advisor to bring these ideas. This is something that we're very well aware of.

Mrs. BICE. Good. And when it—when we're talking about cyber leverage, how does CYBERCOM leverage commercial threat information provider—threat at information providers and how does CYBERCOM share information currently?

I've heard some concerns about not sharing information. You mentioned the FBI previously in a comment that you made.

I think we have siloed a lot of information and there's not as much sharing as there could be. Can you talk a little bit about that?

General NAKASONE. There's a program called Under Advisement. That is a commercial program that we execute at U.S. Cyber Command. It's run by 12 people of my command that reaches out to a number of commercial providers and talks about what we're seeing in cyberspace, and what are you seeing? It's a two-way street, right. I mean, so we're very interested in, obviously, what they're

seeing. But they're also interested to know what are you seeing about our threats.

This is an incredibly and powerful program that has been able to allow us insights into ransomware and insights into adversaries that are seeking vulnerabilities within our networks. But it's all based upon this idea of give and take with the private sector. And so this is a program that I would commend in terms of really great success that we're seeing.

Mrs. BICE. I would love to see more of that because I think that information share is going to be crucial for us to be able to prevent significant national security cyber threat that we face every day. But that sharing of information for the private sector is crucial.

General NAKASONE. If I might follow up. One other piece that I do want to highlight is that I did mention the Federal Bureau of Investigation and our Cyber National Mission Force—it's commanded by Major General Hartman—our elite force that has done tremendous work in defense against malicious cyber actors in both elections and ransomware, is closely partnered with a number of different field offices throughout the United States to share this information.

As you're well aware, the FBI, obviously, has a track on these cyber criminals within the United States. So this pairing of information is one of the areas that Director Wray and I talk about a lot as being a significant success story in 2021.

Mrs. BICE. Thank you, Mr. Chairman. I yield back.

Mr. LANGEVIN. Thank you, Mrs. Bice.

We're going to be wrapping up in just a minute to go into the closed session upstairs. But before we do that, General Nakasone, if I could, earlier today in your appearance in front of the Senate Armed Services Committee you spoke to the—to readiness matters and in those remarks you noted there are defined roles for Cyber Command and the military services, and that the services, generally, are able to present forces that have passed through a basic level of training.

From there, it's the command's responsibility to manage the advanced training. I know that in discussions that you and I have had, that obviously training is important, having the—you know, the right skill level, especially as you're operating—our operators operating in cyberspace.

If we have got concerns around the readiness of our force and the commitment of the services to the cyber domain writ large, should we be pressing the services to reexamine and consider raising the bar on what that basic level of training consists of and is defined as? Or, you know, do you recommend a better way of doing this, should we be taking a fresh look at that?

General NAKASONE. Chairman, I mean, you've hit the nail on the head here. This is what we're doing right now, which is, the Secretary of Defense has signed out a memorandum directing that one service, the Army, has the responsibility for advanced cyber training.

And so now we're going to build that with the Army being in charge to be able to ensure that we have standards at different locations for this training.

My hope is that by the time an operator comes to me, there's very little training that they have to do. That's not the case today for a number of different reasons, and so, again, this is part of our maturity, our readiness. But I do see progress, as we move forward.

Mr. LANGEVIN. I hope you'll have advice for us and thoughts on how we kind of make that—the training kind of uniform level of readiness among all the services so when they get to you, you know, they're at peak level and then you can take them, obviously, even further. So—

General NAKASONE. And part of this, Chairman, is, you know, cyberspace is one of the few domains that is just now getting a simulation capability. For us it's called a Persistent Cyber Training Environment.

It's where we're able to do missions in a simulated way, and you can imagine the power of this being able to do with training, repetition and repetition and more reps, being able to do that.

So we're deploying that now throughout our service elements to be able to do that. That's a key enabler that we need to be able to do in 2022.

Mr. LANGEVIN. Excellent. Excellent. And I know that, you know, we have talked about the amount of time they're assigned to U.S. Cyber Command in a cyber role and, you know, before we wrap up is there anything that you want to talk about, you know, publicly in terms of how long you'd like to keep them, you know, doing cyber work as opposed to the current construct? Anything you want to add?

General NAKASONE. Forever.

[Laughter.]

Mr. LANGEVIN. So I—

General NAKASONE. So, I mean, Chairman, I would say that I'm working this very closely with the service chiefs now. In fact, I'm in communication with them to look at this. This is something that Command Sergeant Major Lyon is also working with the senior enlisted leaders.

We have to standardize tour lengths. We need to standardize Active Duty service obligations. We need to take a look at a means upon which we have, I think, more uniformity with regards to how long, you know, young men and women are going to be with our force.

Mr. LANGEVIN. Agreed. That's something that I and the committee is going to continue to follow. I look forward to working with you on that, going forward, as well.

Okay. So with that, I'm going to ask unanimous consent that Ranking Member Banks' opening statement be entered into the record. He's still in his markup. And so without objection, so ordered.

[The prepared statement of Mr. Banks can be found in the Appendix on page 32.]

Mr. LANGEVIN. With that, I want to thank members for their questions. I want to thank our witnesses for their testimony today and their answers to the questions.

Members may have additional questions that they need to get answered that will be submitted for the record. We ask that you respond to those members in writing as expeditiously as possible.

We will now adjourn and move to the closed session upstairs.

With that, the subcommittee stands adjourned.

[Whereupon, at 5:27 p.m., the committee proceeded in closed session.]

A P P E N D I X

APRIL 5, 2022

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

APRIL 5, 2022

Chairman James R. Langevin
Cyber, Innovative Technologies, and Information Systems Subcommittee
“Operations in Cyberspace and Building Cyber Capabilities Across the
Department of Defense”
April 5, 2022

The subcommittee will come to order. Welcome to today’s hearing, “Operations in Cyberspace and Building Cyber Capabilities Across the Department of Defense”. We have convened this as a hybrid hearing and are joined by Members who are participating remotely. Members who are joining remotely must be visible onscreen for the purposes of identity verification, establishing and maintaining a quorum, participating in the proceeding, and voting. Those Members must continue to use the software platform’s video function while in attendance, unless they experience connectivity issues or other technical problems that render them unable to participate on camera. If a Member experiences technical difficulties, they should contact the committee’s staff for assistance.

Video of Members’ participation will be broadcast in the room and via the television/internet feeds. Members participating remotely must seek recognition verbally, and they are asked to mute their microphones when they are not speaking.

Members who are participating remotely are reminded to keep the software platform’s video function on the entire time they attend the proceeding. Members may leave and rejoin the proceeding. If Members depart for a short while, for reasons other than joining a different proceeding, they should leave the video function on. If Members will be absent for a significant period, or depart to join a different proceeding, they should exit the software platform entirely and then re-join it if they return. Members may use the software platform’s chat feature to communicate with staff regarding technical or logistical support issues only.

I have designated a committee staff member to, if necessary, mute unrecognized Members’ microphones to cancel any inadvertent background noise that may disrupt the proceeding.

I’d like to welcome our witnesses:

- **General Paul Nakasone**, the Commander of U.S. Cyber Command and the Director of the National Security Agency,
- and **Dr. John Plumb**, who was recently confirmed as the Assistant Secretary of Defense for Space Policy, and who will serve concurrently as the Principal Cyber Advisor to the Secretary of Defense.

Dr. Plumb appeared in front of the Intelligence & Special Operations Subcommittee on Friday, so this is only his second appearance as a witness for the House Armed Services Committee, and the first on matters related to cyber issues. John, I understand you’re a proud Notre Dame alum, I know that Ranking Member Banks is extremely happy to hear this, and I promise not to hold it against you! General Nakasone, it is always great to see you. I have valued our relationship for

many years, and I admire your dedication to both your mission, and your people. We warmly welcome both of you to today's proceedings and look forward to working together.

As I'm sure you've heard by now, I plan on retiring at the end of the 117th Congress. After nearly 22 years in Congress, I am ready to chart a new course, and have cherished my time serving the people of Rhode Island's Second District, and our women and men in uniform. And over the course of my tenure, I have seen cybersecurity and cyber issues move from the periphery to the center of national security. I hope that I've played some small role in focusing the Congress on these vital matters.

Out of curiosity, I looked back at prior years' National Defense Authorization Acts. In 2001, my first year in Congress, the NDAA didn't even mention the words "cyber" or "internet", not even once.

Compare that to last year alone, where not only does the word "cyber" appear much more than once, but it is the second consecutive year where there is an entire chapter, or "title" of the NDAA, devoted to cyberspace-related matters.

In the three years that I have served as Chairman of this Subcommittee, we have had more than 220 separate pieces of legislation, across three NDAs, enacted into law. This Subcommittee, along with our colleagues from the Senate, have tackled:

- cybersecurity of weapons systems;
- cyberwarfare personnel pay parity;
- cyber targeting;
- support to the private sector and critical infrastructure;
- capabilities to defeat ransomware;
- budgetary authorities;
- cyber requirements for defense contractors;
- and, of the most significance to me, the creation of the National Cyber Director role in the Executive Office of the President.

We no longer have to debate whether we will fight wars in cyberspace, and to some, it may seem crazy that we ever had to have that discussion in the first place. Cyberspace is a recognized domain of warfare, and for better or worse, our service members and civilians are engaged with our adversaries on a daily basis.

Over that same period, the Department of Defense and the military Services have undergone a similar transformation in this space... We have a dedicated Combatant Command for cyberspace operations. We have Soldiers, Sailors, Airmen, Marines, Guardians, and Coast Guardsmen defending our nation in cyberspace. And, we have witnessed the incredible outcomes for our national defense that we can create through cyber means.

And yet, for all the progress that we've made on this front, there can be a sense of déjà vu in the issues we have to address. On workforce matters, for instance, the points we can and should make today are unnervingly similar to what

was said in hearings 10, 15, and even 20 years ago. Statements such as “we struggle in competing with the private sector for talent”, or “there remains a critical shortfall in our cyber talent”. Since 2010, this body has legislated on cyber and STEM workforce issues through 55 provisions, and sometimes, we seem no closer than we were before.

We continue to struggle in elevating considerations for the cyber domain to a level commensurate with how we treat the land, air, sea, and now, space domains. I have been in Congress long enough to know that progress with any important issue is always incremental; however, *incremental does not have to be synonymous with glacial*.

The responsibility of legislators is tremendous, and we wield the tools at our disposal as carefully as possible. When an issue requires attention, we are judicious in how we direct the Department to respond. Directive actions are powerful, but resorting to these too frequently lessens their effect. That is why we often direct other actions, such as: reports, briefings, quarterly updates, implementation plans, designation of senior officials, and many, many others. We use these to make clear the view of Congress.

We use these tools because they are often successful in accomplishing the desired end state. It is not an exaggeration to say that we have tried to use these alternatives hundreds of times in the cyber context. However, at a certain point, when we are discussing the same issues as our predecessors’ predecessors, we have to ask ourselves: “can we continue trying the same types of approaches that don’t result in change?”

If we are repeating the same frustrations on an annual basis — about cybersecurity of the Defense Industrial Base, or the readiness of our cyber forces, or the way in which the Department manages cyber issues — then at some point, we must acknowledge a lack of preparedness to address these critical challenges.

Congress has a great obligation to national security. During my final year in these halls, I am not interested in allowing my successor to inherit the same challenges that plague us today. I look forward to being bold, to pushing for overdue changes, and to working collaboratively with our Members and our witnesses.

With that, I want to again thank our witnesses for appearing before us today. As a reminder, after this open session, we will move to Rayburn 2212 for a closed Member-only session.

I’ll now turn to Ranking Member Banks for his remarks.

Statement of Hon. Jim Banks
Ranking Member, Subcommittee on Cyber, Innovative Technologies,
and Information Systems
Hearing on
Operations in Cyberspace and Building Cyber Capabilities
Across the Department of Defense
April 5, 2022

Thank you, Chairman Langevin.

General Nakasone and Dr. Plumb, thank you for being here today. I look forward to our conversation because the cyber domain is vital to the United States' security today and in the future.

Cyber is a linchpin.

It cannot and should not be an afterthought; cyber is not a magic dust to be sprinkled on a conflict when our tanks, ships and planes have failed.

The Department of Defense must make significant cyber investments with an appreciation of the difficulties and costs it will take to find solutions.

Not only do we need sustained investments in our cyber workforce, capabilities, tools, and defenses, we need everyone from the Secretary of Defense to the combatant commands, to the military departments, to every warfighter and civilian to appreciate the importance and impact of cyber.

We must understand that cyber is not confined to computers and phones, but that it can have devastating effects on our weapons, vehicles, command and control, and intelligence or on our water supply, electricity, and logistics.

Cyber needs to be cultivated both as a capability for our forces on the battlefield and as a tool to protect our networks, beginning in research and development, to acquisition and sustainment, and in operations.

It would be naïve to think our adversaries are not seeking every advantage in this domain to keep us out of their spheres of influence. Why engage in a fight they will lose, if through cyber they can prevent us from ever being able to fire a shot?

I realize that no one in the Department knows these facts better than you, General Nakasone. I am concerned that cyber can get lost in a scrum of all the competing priorities in the department, and I am committed to ensuring that you have the authorities, capabilities, and resources you need to succeed not just in the cyber domain, but in any of the department's missions that CYBERCOM is asked to support.

The cyber workforce is foundational to our strength. We need to be attracting, training, and retaining the men and women who make up our cyber teams, especially as you field more teams. Force readiness is key in succeeding in our mission. I think our cyber teams will be in higher demand in the years ahead and they must be ready to defeat the threats our adversaries pose.

Cyberspace, as a war-fighting domain, does not fit neatly into our definitions of peacetime or kinetic warfare. We need to be thinking about how our adversaries

are using cyber to gain advantages over the United States and make sure that CYBERCOM is postured to meet the threats.

I believe this requires a fundamental shift in how we man, train and equip the military. It requires the department to think strategically and acknowledge that the cyber domain does not look like the air, land, or sea domains that have been dominant in our past.

It is not going to be an easy task, but I look forward to working with you both to ensure our warfighters never enter a fair fight.

STATEMENT OF
THE HONORABLE DR. JOHN PLUMB
ASSISTANT SECRETARY OF DEFENSE FOR SPACE POLICY
TESTIMONY BEFORE THE
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON CYBERSECURITY, INNOVATIVE TECHNOLOGIES, AND
INFORMATION SYSTEMS
APRIL 5, 2022

Introduction

Thank you Chairman Langevin, Ranking Member Banks, and Members of the Subcommittee. I am pleased to join General Nakasone, Commander of U.S. Cyber Command (USCYBERCOM), to report on the progress the Department of Defense (DoD) has made in achieving the Department's objectives in cyberspace.

To start, I would like to offer some perspective on the current strategic context. In 2021, as the country and the world continued to grapple with the new normal created by the COVID-19 pandemic, increasingly relying on the internet for business, social, and economic activities, we saw cyber actors conduct malicious cyber activities at an unprecedented scale and in creative ways to advance their interests. The Federal Government and numerous private sector entities grappled with the aftermath of the Russia-led exploitation of SolarWinds software, first discovered in December 2020, by which Russia compromised dozens of networks. In March 2021, Microsoft discovered a vulnerability in its Microsoft Exchange servers that the Chinese group Hafnium used to compromise thousands of networks. And in May 2021, a ransomware operation affecting systems impacting Colonial Pipeline's operations led to a temporary halt in the company's fuel distribution along the East Coast of the United States.

But 2021 also demonstrated that the Department, the U.S. Government, and our private sector partners are determined to find creative ways to work together to mitigate cyber vulnerabilities and combat cyber threats. The Department of Justice—both Main Justice and the FBI—took unprecedented measures to help victims of the Hafnium attacks from further exposure. The President signed an Executive Order in April 2021, imposing sanctions on Russian individuals and entities, and expelling several Russian officials in response to Russia's malign cyber activities, including the SolarWinds intrusion and its efforts to interfere in U.S.

elections and democratic institutions. Late in 2021, when a vulnerability was discovered in Apache's Log4j software, the Department moved quickly not only to determine the implications of the vulnerability for its own network, but also to share useful information with interagency and private sector partners.

The U.S. Government and private sector have also collaborated in unprecedented ways to monitor and prepare for potential Russian cyberattacks against the homeland and our NATO Allies amidst Russia's unlawful invasion of Ukraine. The Department of Defense has played a supporting role in these whole-of-government efforts. The Department is also a full participant in interagency domestic preparedness efforts and has issued numerous alerts and shared threat information with foreign allies and partners, Defense Industrial Base entities, and interagency partners.

For its own DoD Information Network (DODIN), the Department constantly works to uncover potential network vulnerabilities and enhance its defense. DoD has been working tirelessly to enhance and harden the cybersecurity posture of its own networks as well as the networks of the Defense Industrial Base. DoD also continues to implement the various facets of the Biden Administration's Executive Order for Improving the Nation's Cybersecurity, such as zero trust architecture. These cybersecurity efforts are complementary to the institutional reforms currently underway to improve DoD's digital presence including cryptography modernization, migration to a secure cloud, strengthening our artificial intelligence capabilities, and expanding the use of data analytics.

Current Threat Environment

As Secretary Austin has made clear, the People's Republic of China (PRC) is the pacing challenge for the Department, including in cyberspace. PRC leaders believe that achieving

information dominance in cyberspace will enable China to seize and maintain the strategic initiative in a crisis or conflict. Therefore, the PRC is rapidly advancing and integrating its cyber capabilities to disrupt our ability to mobilize, project, and sustain the joint force. The PRC's malicious cyber campaigns include exfiltrating sensitive information from U.S. public and private sector institutions and stealing U.S. intellectual property and research from the defense industrial base. The need for, and challenges of, establishing meaningful dialogue with China on norms of behavior in cyberspace is clear: despite President Obama's and President Xi Jinping's 2015 joint commitment not to conduct or knowingly support cyber-enabled intellectual property theft, PRC malicious cyber activity continues unabated.

While the PRC is unequivocally the Department's pacing challenge, Russia, as evidenced by its brutal and unlawful invasion of Ukraine, is the near-term threat. Cyber operations are a key component of Russia's wartime strategy. In addition to offensive military operations against Ukraine, Russian military and intelligence forces are targeting Ukrainian networks to collect intelligence and spread disinformation.

Russia's persistent campaigns in and through cyberspace pose a long-term strategic risk to the United States, our allies, and our partners. Russia's brazen cyberattacks against Ukrainian critical infrastructure, its disinformation campaigns and election interference in 2016 and 2020, and its disruptive SolarWinds campaign all demonstrate Russia's willingness to employ malicious cyber activities to disrupt targets and destabilize democratic processes. They also demonstrate the breadth of Russia's cyber espionage capabilities and expertise.

Like China, Russia could also engage in disruptive cyber attacks against U.S. critical infrastructure to distract the United States, impose costs on the American people, or complicate the Department's operations or mobilization as a prelude to armed conflict.

While not at the level of the PRC or Russia, Iran and Democratic Republic of Korea (DPRK) also employ increasingly sophisticated cyber capabilities that ultimately threaten U.S. interests. Iran conducted cyber-enabled influence campaigns to intimidate and influence American voters during the 2020 U.S. presidential election, and has previously targeted U.S. critical infrastructure. The DPRK has conducted cyber-enabled theft of fiat currency and cryptocurrency to generate revenue for the regime, including for its weapons of mass destruction and ballistic missile programs.

Finally, ransomware criminals—whether totally independent from, tacitly tolerated by, or actively encouraged by nation states—remain a persistent threat to U.S. interests. The malicious activities of these non-state actors affect the material well-being of American citizens and corporations by disrupting their operations, extracting ransoms, and stealing their resources. The volume and scope of the disruptive activities of ransomware actors has irrevocably altered the strategic environment. President Biden has made it a priority to address ransomware threats. The Department continues to devote people, technology, and expertise to generate insights and options against ransomware actors in support of whole-of-government efforts to combat this threat.

Offensive Authorities

The Department recognizes the need to prioritize missions to disrupt threats overseas at their source in and through cyberspace. In a domain subject to constant change, our success in this mission requires the ability to conduct timely offensive cyber operations when threats meet the threshold for action, as established in policy. The existing national policy framework, NSPM-13, enables the Department's offensive cyber operations, and has made important and positive contributions to the Department's ability to engage the threat. The Department will

continue to advance and modernize how we operate in cyberspace to effectively engage cyber threats with the necessary speed and agility in a well-coordinated manner.

The Department's superiority in the cyber domain depends on maintaining an ability not only to move quickly, but also in a cohesive manner with key partners. The collaboration between the National Security Agency and U.S. Cyber Command has been a significant enabler of that success. Therefore, I am committed to ensuring that any future decision regarding the so-called "dual-hat" arrangement, in which the Director of the National Security Agency is also the Commander of U.S. Cyber Command, protects our national security interests and advances the Department's progress in cyberspace.

Cybersecurity of Partners and Allies

The U.S. network of allies and partners is an asymmetric advantage that our adversaries cannot hope to match. But that network is vulnerable to cyber intrusions and exploitation. Poor cybersecurity threatens our allies' and partners' military capabilities and their ability to safeguard sensitive information. It consequently also impedes our ability to train and exercise with them, or plan and execute joint military operations with them.

Enhancing the cybersecurity capabilities and defenses of key allies and partners in order to improve cooperation and preparedness across all warfighting domains is therefore a priority for the Department. We will accomplish this through a combination of training, equipping, and enabling select allies and partners to implement sound cybersecurity solutions. Our consistent message to allies and partners is that we have a shared interest in their cybersecurity and cyber defenses, which affects our collective ability to operate. We also emphasize the need for continuous vigilance against cyber threats: merely remediating known vulnerabilities is not sufficient.

In the Indo-Pacific region, we are working closely with our allies and partners, such as Japan, the Republic of Korea, Taiwan, Singapore, India, and others to defend themselves against malicious intrusions into their various defense networks. Our activities include bilateral dialogues, training, cyber education courses, and cyber exercises, including CYBER BLADE with Japan and CYBER HELIX with Singapore. We also plan to include Indo-Pacific region partners and allies into the USCYBERCOM-hosted CYBER FLAG later this year.

In Europe, we look forward to the next iteration of CYBER FLAG in July, which will incorporate NATO Allies and other European partners and aims to improve the overall capability of the United States and its allies to respond in unison to defend against malicious activities in and through cyberspace.

While the Department is committed to assisting its partners, it does not have the capacity to do so alone. Close collaboration between the private sector and our U.S. government interagency partners is required to fill the demand for cybersecurity training and capacity building. Our U.S. defense industrial base partners have an opportunity to assist by increasing their offerings in cyber training and education abroad.

Cyber Posture Review and Cyber Strategy

Pursuant to section 1644 of the National Defense Authorization Act for Fiscal Year 2018, as amended, the Department is currently conducting its 2022 Cyber Posture Review (CPR), an assessment of the Department's organizations, plans, programs, and policies germane to cyber operations. The posture review focuses in particular on USCYBERCOM, the Cyberspace Operations Forces, and supporting elements in the force generation, intelligence, and acquisition communities across the Department of Defense.

Once complete, the Cyber Posture Review will inform the Department's 2022 Cyber Strategy. The strategy will provide guidance to the Department as to how its cyber combat power will be used to implement the National Defense Strategy and how, in particular, cyber operations will advance integrated deterrence. The strategy will also identify potential solutions and paths forward for addressing any gaps identified in the posture review.

The 2022 Cyber Strategy will build on the strengths of the 2018 Cyber Strategy—particularly its focus on taking proactive action to counter cyber threats—while expanding our approach to domestic and international partnerships, recognizing the human dimension of cyber competition, and grappling with the changes we have seen to the cyber threat environment in the last four years.

Taken together, the Cyber Posture Review and DoD Cyber Strategy should propel the maturation of USCYBERCOM, the Cyberspace Operations Forces, and the entire DoD cyber enterprise, as well as the personnel, processes, and systems across the Joint Force that operate in, rely on, or interact with cyberspace.

Conclusion

Our potential adversaries continue to evolve their approaches and routinely use their cyber capabilities in competition and conflict to seek political, economic, information, and military advantages. DoD's ability to successfully operate in cyberspace is therefore absolutely essential to U.S. national security. I look forward to working with the committee as we seek to strengthen both our defensive and offensive cyber capabilities and mature our cyber forces. Thank you for your continued dedication to the Department and the nation. I look forward to your questions.

Dr. John F. Plumb
Assistant Secretary of Defense for Space Policy

Dr. John F. Plumb was confirmed in March 2022 as the first Assistant Secretary of Defense for Space Policy. In this role he is responsible for the overall supervision of policy for the Department of Defense for space warfighting. His policy portfolio encompasses the Department's strategic capabilities for integrated deterrence: space, nuclear weapons, cyber, missile defense, electromagnetic warfare, and countering weapons of mass destruction. He also serves as the Principal Cyber Advisor to the Secretary of Defense.

Dr. Plumb has served in various national security roles both in and out of uniform for nearly three decades. As an active duty US Navy submarine officer, he served on a fast attack Los Angeles- class submarine and as an instructor at the Navy's nuclear power school. He then transitioned to the Navy reserves, commanding eight different reserve units over 20 years. As a civilian he held previous roles in the Senate, the Pentagon, and on the National Security Council staff at the White House. Prior to his confirmation he spent several years working for Federally Funded Research and Development Centers, first as a Senior Engineer at the Rand Corporation, and then as Principal Director, Chief of Government Relations for the Aerospace Corporation.

He holds a B.S. in Physics from the University of Notre Dame, and an M.S. in Physics and Ph.D. in Aerospace Engineering from the University of Colorado. His academic awards include the University of Notre Dame Student Leadership Award and an American Association for the Advancement of Science (AAAS) Congressional Science & Technology Fellowship sponsored by the Institute of Navigation. His personal military decorations include the Legion of Merit, the Meritorious Service Medal, and the Navy Commendation Medal. His civil service awards include the Office of the Secretary of Defense Exceptional Public Service Award, the Department of State Superior Honor Award, and the Secretary of Energy Achievement Award.

UNCLASSIFIED

POSTURE STATEMENT OF
GENERAL PAUL M. NAKASONE
COMMANDER, UNITED STATES CYBER COMMAND
BEFORE THE 117TH CONGRESS
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES AND
INFORMATION SYSTEMS

APRIL 5, 2022



UNCLASSIFIED

UNCLASSIFIED

(U) Chairman Langevin, Ranking Member Banks and distinguished members of the Committee, thank you for your enduring support and the opportunity today to represent the hard working men and women of U.S. Cyber Command (USCYBERCOM). I am honored to be here and testify beside Assistant Secretary of Defense John Plumb.

(U) Let me begin by acknowledging the dedicated service of our Service members and civilians at USCYBERCOM. Their mission is to plan and execute global cyber operations, activities, and missions to defend and advance national interests in collaboration with domestic and international partners across the full spectrum of competition and conflict. Our three lines of operation are to:

- Provide mission assurance for the Department of Defense by directing the security, operation and defense of Department of Defense Information Network (DODIN), including DoD's critical infrastructure;
- Help deter and defeat strategic threats to the United States and its national interests; and
- Assist Combatant Commanders to achieve their objectives in and through cyberspace.

(U) U.S. Cyber Command directs operations through its components. These include the Cyber National Mission Force-Headquarters (CNMF-HQ), Joint Force Headquarters-DoD Information Network (JFHQ-DODIN, the commander for which is dual-hatted as the Director of the Defense Information Systems Agency) and Joint Task Force Ares. They work with our Joint Force headquarters elements, the commanders for which are dual-hatted with one of the Services' cyber components (Army Cyber Command, Marine Corps Forces Cyberspace Command, Fleet Cyber Command/Tenth Fleet, Air Force Cyber/16th Air Force and Coast Guard Cyber Command). The Command currently comprises 133 teams across the Cyber Mission Force (CMF), approximately 6,000 Service members, including National Guard and Reserve personnel on active duty. The CMF is due to grow by 14 teams over the next five years.

(U) USCYBERCOM is postured to execute its missions and meet both the nation's near-term and enduring strategic challenges in cyberspace. I shall address the Command's role in the crisis caused by Russia's invasion of Ukraine, and then speak to our preparedness for persistent threats and in meeting our long-term pacing challenge, China. As the Commander of USCYBERCOM and Director of the National Security Agency (NSA), I have learned that the Command's linkage with NSA is essential to achieving critical outcomes for the nation in both cyber and intelligence operations. The dual-hatted command relationship improves planning, resource allocation, risk mitigation, and unity of effort. It allows us to operate with speed, agility, and mission effectiveness that we could not achieve without it. This is critical to meeting the strategic challenges of our adversaries as they grow in sophistication, aggressiveness and scope of operations.

(U) Strategic Challenges

(U) Russia's invasion of Ukraine demonstrated Moscow's determination to violate Ukraine's sovereignty and territorial integrity, forcibly impose its will on its neighbors and

UNCLASSIFIED

challenge the North Atlantic Treaty Organization (NATO). Russia's military and intelligence forces are employing a range of cyber capabilities, to include espionage, influence and attack units, to support its invasion and to defend Russian actions with a worldwide propaganda campaign.

(U) U.S. Cyber Command (with NSA) has been integral to the nation's response to this crisis since Russian forces began deploying on Ukraine's borders last fall. We have provided intelligence on the building threat, helped to warn U.S. government and industry to tighten security within critical infrastructure sectors, enhanced resilience on the DODIN (especially in Europe), accelerated efforts against criminal cyber enterprises and, together with interagency members, Allies, and partners, planned for a range of contingencies. Coordinating with the Ukrainians in an effort to help them harden their networks, we deployed a hunt team who sat side-by-side with our partners to gain critical insights that have increased homeland defense for both the United States and Ukraine. In addition, USCYBERCOM is proactively ensuring the security and availability of strategic command and control and other systems across the Department. We have also crafted options for national decision makers and are conducting operations as directed.

(U) When Moscow ordered the invasion in late February, we stepped up an already high operational tempo. We have been conducting additional hunt forward operations to identify network vulnerabilities. These operations have bolstered the resilience of Ukraine and our NATO Allies and partners. We provided remote analytic support to Ukraine and conducted network defense activities aligned to critical networks from outside Ukraine – directly in support of mission partners. In conjunction with interagency, private sector and Allied partners, we are collaborating to mitigate threats to domestic and overseas systems.

(U) These measures were made possible by the patient investments in cyberspace operations capabilities and capacity over the last decade, as well as by the lessons that we as a Department and a nation have learned from operational experience. The current crisis is not over, but I am proud of the response of our people and confident in their ability to deliver results no matter how long it lasts. Their grit and ingenuity have been inspiring.

(U) Shifting to longer-term considerations, I note that our operations are planned and executed in accord with the *Interim National Security Strategic Guidance*. Underpinning our work is Integrated Deterrence. We provide combat-capable forces in cyberspace that engage in active campaigning to disrupt adversary actions, demonstrate capabilities and resolve, shape adversary perceptions and gain warfighting advantages should deterrence fail. Integrated Deterrence is multi-partner, multi-domain, multi-theater and multi-spectrum, requiring us to compete every day in cyberspace against military and intelligence actors seeking to undermine our nation's strength and strategic advantages.

(U) Cyberspace is a dynamic and inter-connected domain where near-peer adversaries seek to exploit gaps and seams between our organizations and authorities. Such adversaries use a variety of cyber means to compromise our systems, distort narratives and disseminate misinformation. These actions threaten our national interests by impairing the safety and security of our citizens, stealing intellectual property and personal information while seeking to

UNCLASSIFIED

undermine the legitimacy of our institutions. Our adversaries have demonstrated sophisticated cyber-attack capabilities for use in competition, crisis and conflict, but I am confident that USCYBERCOM is well postured to meet those challenges.

(U) China is our pacing challenge, which I see as both a sprint and a marathon. China's military modernization over the past several years threatens to erode deterrence in the western Pacific, which requires immediate steps to redress. At the same time, China is an enduring strategic challenge that is now global in scope. Beijing is exerting influence worldwide through its rising diplomatic, informational, military, and economic power. China is a challenge unlike any other we have faced. I have therefore created a China Outcomes Group under joint USCYBERCOM and NSA leadership to ensure proper focus, resourcing, planning, and operations to meet this challenge. Although we recognize that much of our effort will be in support of U.S. Indo-Pacific Command, China is a global challenge. The success of our efforts will depend in part on the resilience and capabilities of regional and worldwide partners. We are building operating relationships and also dedicating long-term work to enhance their cybersecurity and cyberspace operations forces.

(U) Iran and North Korea are cyber adversaries growing in sophistication and willingness to act. Despite our strengthened focus on China, we are maintaining our ability to counter these threats. Tehran has increased ransomware operations, the targeting of critical infrastructure, and influence campaigns (including in our 2020 elections). We support U.S. Central Command in its efforts against Iranian-backed proxies in Iraq and Syria (as we also did in the withdrawal from Afghanistan last summer). North Korea uses its cyber actors to generate revenue through criminal enterprises, such as hacking-for-hire and theft of cryptocurrency. USCYBERCOM works with the Departments of State and Treasury to stem Pyongyang's campaigns.

(U) The scope, scale and sophistication of these threats is rising. The United States faced major cybersecurity challenges over the last year, beginning with the SolarWinds supply-chain compromise but extending to incidents involving software compromises that affected companies like Colonial Pipeline, Microsoft, JBS, Kaseya, and Apache. In each instance, our Command worked through CNMF and other components to provide insights to our homeland security and law enforcement partners, who are the nation's first line of defense for U.S. systems and networks.

(U) Ransomware can have strategic effects as America saw in the disruption of Colonial Pipeline's systems. CNMF has taken numerous actions over the past year to combat ransomware in close partnership with law enforcement, interagency, industry, and foreign partners to disrupt and degrade the operations of ransomware groups attacking our nation's critical infrastructure. CNMF and NSA enabled whole-of-government actions targeting ransomware actors, passing key insights in near-real time. CNMF was a key partner in the whole-of-government effort to disrupt and impose costs against those who targeted Colonial Pipeline.

(U) USCYBERCOM (with JFHQ-DODIN) also defended the DODIN against cyber threats and helped ensure that disruptions to its systems and data remained inconsequential and brief. We continue to innovate in enhancing DODIN defenses and countering adversary threats; indeed, we must, because our adversaries are agile and adaptive. Key to this effort is building

UNCLASSIFIED

resilience in our systems and platforms while preparing the Department, the other Combatant Commands and Defense Industrial Base (DIB) companies to operate even in degraded cyber environments.

(U) U.S. Cyber Command Posture for the Future

(U) Our success against these growing challenges is a result of sustained efforts and investments, not to mention a lot of hard work. I should add that that work over the last two years took place under COVID-19 mitigations. USCYBERCOM has been on-mission, running operations and exercises with the joint force and domestic and foreign partners throughout the pandemic, with negligible workforce transmission and slight impact to operations. We will continue to prioritize workplace safety, workforce confidence, and mission continuity.

(U) We see 2022 as a year of opportunity to make progress in several areas that will enhance USCYBERCOM's capabilities and contributions to national security. With this in mind, I have established the following priorities for our Command:

- Readiness;
- Operations in Defense of the Nation;
- Integrated Deterrence;
- Recruiting, Retention and Training; and
- Joint Cyber Warfighting Architecture and Enhanced Budget Control

(U) Readiness is priority one. It is foundational to the success of operations in defense of the nation and Integrated Deterrence. USCYBERCOM has made progress despite challenges. We improved our ability to monitor the status of our cyber mission forces down to the team, mission element and individual levels. Across the Department, USCYBERCOM is responsible for setting standards for all of DoD's Cyberspace Operations Forces. We work to provide commanders with the situational awareness they require to assess risks and make informed decisions, not just in operations but in maintaining force readiness as a whole. We will work with the Services this year to ensure the progress we have made over the past year continues.

(U) Second, along with our interagency partners, we defended the nation's recent elections against foreign interference and are preparing to support the defense of this year's midterms through the combined efforts of USCYBERCOM and NSA. We anticipate that our adversaries will continue using their military and intelligence elements to affect our democracy. Thus I appointed a USCYBERCOM general officer and an NSA senior executive to oversee election security in 2022. This is an enduring, no-fail mission for USCYBERCOM.

(U) Interagency partnerships are crucial in these efforts. Working with the Federal Bureau of Investigation (FBI) and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has demonstrated that we are much stronger together. Indeed, no single agency can defend the nation on its own. USCYBERCOM imposes costs on threat actors and provides insights to domestic and foreign partners to mitigate and respond to malign activity, enabling each to act under its respective authorities. We will continue to

UNCLASSIFIED

collaborate with our domestic partners across the federal government and the states to share best practices and expertise.

(U) Our adversaries also target our economy. DIB companies are on the frontlines in cyberspace and are constantly targeted by malicious cyber actors. Over the past year, we have deepened our relationships with private industry through voluntary information sharing. Since the nation's critical infrastructure and systems are largely in private hands, these relationships have directly enhanced our operations, in addition to the security of their commercial systems.

(U) Third, supporting the national priority of Integrated Deterrence means preparing for crisis and conflict while campaigning in competition across the full spectrum of cyber operations. It also means building the strategic partnerships that enable the defense of U.S. systems and networks beyond the DODIN and the DIB. Our foreign partnerships begin with our "Five Eye" Allies – the United Kingdom, Canada, Australia and New Zealand. The circle of partnership has been enlarged in recent years as we enhanced existing relationships with allies and forged new ones with several nations, especially in Europe and the Indo-Pacific region.

(U) Fourth is building a skilled workforce through recruitment, training, and retention. Talent is key to preserving our competitive edge against our adversaries. USCYBERCOM has improved its civilian hiring with the use of its congressionally-granted Cyber Excepted Service (CES) authorities, which allow us to offer competitive compensation packages for high-demand expertise. In addition, a diverse, talented workforce that expands equity and inclusiveness is an enduring goal. To recruit and retain a skilled military workforce, we are also grateful for the authorities Congress has granted the Services to offer flexible promotion and commissioning avenues in support of the CMF.

(U) Partnerships with academia will aid in engaging the future cyber workforce and enriching the strategic dialogue about cyber. Our new Academic Engagement network began last year and comprises 93 institutions, including 10 minority-serving institutions, across 40 states and the District of Columbia, as of March 25, 2022. Interest in partnering with USCYBERCOM is strong and growing.

(U) Training and proficiency are improving through our mission simulation capabilities, particularly the Persistent Cyber Training Environment (PCTE). The PCTE is helping us mature cyber operations tradecraft, enhance individual proficiencies and enable faster attainment of team certification and collective training in maneuvers such as Exercise CYBER FLAG.

(U) The Reserve Component is critical to protecting the nation in cyberspace. As a result of the partnership between USCYBERCOM and the National Guard Bureau during the 2020 election, Guard units could rapidly share information on malicious cyber activity with state and local authorities. Members of the National Guard and Reserve often have private-sector experience in fields of strong interest to USCYBERCOM. In addition, the ability of the National Guard and Reserve to hire cyber talent has been especially helpful in retaining the contributions of Service members who decide to leave active duty upon completion of their commitment; members can transfer to a part-time status.

UNCLASSIFIED

(U) Our final priority is guiding the Department's investments in cyberspace capability through the Joint Cyber Warfighting Architecture (JCWA) and Enhanced Budget Control. JCWA consolidates and standardizes the Department's cyberspace operations capabilities, enabling us to integrate data from missions and monitoring to help commanders gauge risk, make timely decisions and act against threats at speed and scale. The Department is building JCWA and advancing the Cyber Mission Force's capabilities for conducting the full spectrum of cyberspace operations.

(U) USCYBERCOM is grateful to this Committee and Congress for granting us Enhanced Budget Control over resources dedicated to the Cyber Mission Force. With this authority, USCYBERCOM will improve direction, control and synchronization of investments for cyber operations across the Department of Defense.

(U) *Conclusion*

(U) U.S. Cyber Command views 2022 as a year of significant opportunity for building our capabilities against the five priorities above. Our overarching goal is to build a Command that is ready and capable at providing options and conducting operations in defense of the nation with wider partnerships and world-class talent, all linked through the Joint Cyber Warfighting Architecture. These elements will be essential to our nation's security as it faces an array of adversaries who are expanding the scope, scale and sophistication of their operations against us, and will be critical to developing the right mission posture to meet the unprecedented challenge of China.

(U) The men and women at U.S. Cyber Command are grateful for the support this Committee has given to our Command. We can only succeed with a strong partnership with Congress. Thank you, and now I look forward to your questions.

General Paul M. Nakasone
Commander, U.S. Cyber Command and
Director, National Security Agency/Chief, Central Security Service

General Paul M. Nakasone assumed his present duties as Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service in May 2018.

He previously commanded U.S. Army Cyber Command from October 2016 - April 2018.

A native of White Bear Lake, Minnesota, GEN Nakasone is a graduate of Saint John's University in Collegeville, Minnesota, where he received his commission through the Reserve Officers' Training Corps.

GEN Nakasone has held command and staff positions across all levels of the Army with assignments in the United States, the Republic of Korea, Iraq, and Afghanistan.

GEN Nakasone commanded the Cyber National Mission Force at U.S. Cyber Command. He has also commanded a company, battalion, and brigade, and served as the senior intelligence officer at the battalion, division and corps levels.

GEN Nakasone has served in Joint and Army assignments in the United States, the Republic of Korea, Iraq, and Afghanistan. His most recent overseas posting was as the Director of Intelligence, J2, International Security Assistance Force Joint Command in Kabul, Afghanistan.

GEN Nakasone has also served on two occasions as a staff officer on the Joint Chiefs of Staff.

GEN Nakasone is a graduate of the U.S. Army War College, the Command and General Staff College, and Defense Intelligence College. He holds graduate degrees from the U.S. Army War College, the National Defense Intelligence College, and the University of Southern California.

GEN Nakasone's awards and decorations include the Distinguished Service Medal (with oak leaf cluster), the Defense Superior Service Medal (with three oak leaf clusters), Legion of Merit, Bronze Star, Defense Meritorious Service Medal (with oak leaf cluster), Army Commendation Medal, Joint Service Achievement Medal (with oak leaf cluster), Army Achievement Medal (with four oak leaf clusters), Joint Meritorious Unit Award, Iraq Campaign Medal, Afghanistan Campaign Medal, Combat Action Badge, and the Joint Chiefs of Staff Identification Badge.

GEN Nakasone and his wife are the proud parents of four children, who form the nucleus of "Team Nakasone."

**WITNESS RESPONSES TO QUESTIONS ASKED DURING
THE HEARING**

APRIL 5, 2022

RESPONSE TO QUESTION SUBMITTED BY MR. MOULTON

Dr. PLUMB. The DOD Principal Information Operations Advisor is currently overseeing the review of the DOD Strategy for Operations in the Information Environment and is conducting the first-ever information operations posture review. These and other ongoing efforts will enable DOD to evaluate the effectiveness of our current and planned actions and identify any additional steps that should be considered, including any further organizational adjustments to improve the Department's efficiency and effectiveness. [See page 11.]

RESPONSE TO QUESTION SUBMITTED BY MR. MOORE

General NAKASONE. U.S. Cyber Command missions and authorities dictate that operations will take place outside the United States. As you are aware, legal barriers are but one of the reasons the private sector is reticent to share information with government organizations. Within the United States, the Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) have the responsibility to work with the private sector in regards to protecting their networks and information sharing. Information sharing and public-private partnerships are where the power is—together they both play a vital role in everyone defending and protecting their networks. [See page 13.]

