[H.A.S.C. No. 116–74]

HEARING

ON

# NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2021

AND

# OVERSIGHT OF PREVIOUSLY AUTHORIZED PROGRAMS

BEFORE THE

## COMMITTEE ON ARMED SERVICES
## HOUSE OF REPRESENTATIVES
ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

---

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES HEARING

ON

# THE FISCAL YEAR 2021 BUDGET REQUEST FOR U.S. CYBER COMMAND AND OPERATIONS IN CYBERSPACE

---

HEARING HELD
MARCH 4, 2020

---

U.S. GOVERNMENT PUBLISHING OFFICE
40–605 WASHINGTON : 2020

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

JAMES R. LANGEVIN, Rhode Island, *Chairman*

RICK LARSEN, Washington
JIM COOPER, Tennessee
TULSI GABBARD, Hawaii
ANTHONY G. BROWN, Maryland
RO KHANNA, California
WILLIAM R. KEATING, Massachusetts
ANDY KIM, New Jersey
CHRISSY HOULAHAN, Pennsylvania
JASON CROW, Colorado, *Vice Chair*
ELISSA SLOTKIN, Michigan
LORI TRAHAN, Massachusetts

ELISE M. STEFANIK, New York
SAM GRAVES, Missouri
RALPH LEE ABRAHAM, Louisiana
K. MICHAEL CONAWAY, Texas
AUSTIN SCOTT, Georgia
SCOTT DESJARLAIS, Tennessee
MIKE GALLAGHER, Wisconsin
MICHAEL WALTZ, Florida
DON BACON, Nebraska
JIM BANKS, Indiana

JOSH STIEFEL, *Professional Staff Member*
ERIC SNELGROVE, *Professional Staff Member*
CAROLINE KEHRLI, *Clerk*

# CONTENTS

# THE FISCAL YEAR 2021 BUDGET REQUEST FOR U.S. CYBER COMMAND AND OPERATIONS IN CYBERSPACE

---

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON INTELLIGENCE AND
EMERGING THREATS AND CAPABILITIES,
*Washington, DC, Wednesday, March 4, 2020.*

The subcommittee met, pursuant to call, at 3:26 p.m., in room 2212, Rayburn House Office Building, Hon. James R. Langevin (chairman of the subcommittee) presiding.

## OPENING STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, CHAIRMAN, SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

Mr. LANGEVIN. The subcommittee will come to order.

I apologize to everyone for being late. We just left the Vice President giving a briefing on the coronavirus issue to the Democratic Caucus, but we will get underway.

I want to welcome everyone to today's hearing on the fiscal year 2021 budget request for military operations in cyberspace.

I would first of all like to welcome our witnesses here today.

Mr. Kenneth Rapuano serves as both the Assistant Secretary of Defense for Homeland Defense and Global Security and as the Principal Cyber Advisor to the Secretary of Defense. Prior to returning to government service, Mr. Rapuano worked for federally funded research and development corporations focusing on homeland security and counterterrorism issues.

Mr. Rapuano, welcome back.

Next, General Paul Nakasone serves in three capacities concurrently: Commander, U.S. Cyber Command; also Director of the National Security Agency, and Chief of the Central Security Service. Before his current role, he commanded U.S. Army's Cyber Command and has served as a career intelligence officer through his 33 years in uniform.

General Nakasone, thank you for your service to the Nation, and we are pleased to have you back before the subcommittee once again.

So the Department of Defense created U.S. Cyber Command [CYBERCOM] in 2009, and more than 10 years later we are still working diligently on establishing the foundations, concepts, doctrine, training, and metrics needed to ensure the security of the Nation in the cyberspace domain.

The state of cyber in national defense is more central than ever, and 2020 marks a sea change, with cyber firmly established and accepted as a warfighting domain, capability, and asset. This is highlighted best through the current operational posture and insti-

tutional maturation of CYBERCOM. Over the course of 2020, this subcommittee expects the command to aggressively address issues of readiness, operational tempo, and the defense of the Nation's electoral system, among other things.

This subcommittee has worked to ensure that the Department, the military services, and CYBERCOM are equipped with the tools and authorities necessary to achieve their objectives. In the fiscal year 2020 NDAA [National Defense Authorization Act], we granted new authorities to CYBERCOM and bolstered multiple frameworks for legislative oversight. We seek to balance an appropriate degree of oversight while ensuring the command retains operational flexibility. We will continue this trend through our collective work in the 2021 bill.

CYBERCOM is facing possibly the most challenging year in its existence. General Nakasone, your command sits at the center of the Department's efforts to secure the information environment. The United States faces increasing malicious activity from Russia, Iran, China, and others.

We know about how Russia weaponized information during the 2016 elections, and we must do more to anticipate and counter these sophisticated operations. While we have had some success countering Russia's malign influence campaigns in 2018, we must not let our guard down. We must ensure that we are properly organized within the Department of Defense and coordinating across the United States Government.

I hope you will give us a full assessment of your efforts to protect the country from malign cyber activity. I will be particularly interested to hear how you are working with partners in the interagency to promote a more stable cyberspace and protect our allies' critical infrastructure.

I want to hear, specifically, how you are coordinating and deconflicting activities domestically with the Department of Homeland Security and internationally with the Department of State.

I am also interested to hear from our witnesses about their assessment of CYBERCOM's current force structure.

For the past year, I have had the privilege of serving on the Cyberspace Solarium Commission and want to thank you, in particular, Mr. Rapuano, for your many contributions to our work.

One of the areas of focus of the Commission has been whether CYBERCOM's force structure properly reflects the command's operational aspirations. Essentially, we need to candidly assess whether a force conceived more than 7 years ago is sufficient for a dramatically different environment today. I will also be curious to hear candid assessments on how organic capabilities resident in the services are rationalized with CYBERCOM's mission and strategy.

Throughout our Nation's history, our military has grown accustomed to focusing on the offensive systems, forces, and platforms that deliver effects against our adversaries. Given our geographic advantage of two oceans and our history of primarily fighting overseas, we are conditioned to fight offensively. However, in a connected world with an inestimable number of internet-connected devices, networks, vehicles, and systems, our defensive posture in the cyber domain has never been more critical.

So, while I fully support CYBERCOM's more offensively postured construct, I am concerned that the President's fiscal year 2021 cyber budget signals in select places that we can sacrifice defensive programs and investments in favor of investments in offensive cyber systems and programs.

So I hope that the witnesses will speak candidly about balancing resources to ensure the Department is best postured to protect the United States in cyberspace, whether through defensive or offensive missions.

So, with that, I want to thank our witnesses for appearing before us today. I thank you for all that you are doing on behalf of the country to keep all of us safe.

As a reminder, after this open session, we will move to room 2337 for a closed, member-only session.

With that, I will now turn to Ranking Member Stefanik for her remarks.

[The prepared statement of Mr. Langevin can be found in the Appendix on page 21.]

**STATEMENT OF HON. ELISE M. STEFANIK, A REPRESENTATIVE FROM NEW YORK, RANKING MEMBER, SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES**

Ms. STEFANIK. Thank you, Chairman Langevin.

Secretary Rapuano and General Nakasone, welcome back to this committee.

We are now 2 years removed from U.S. Cyber Command reaching full operational capability. In that time, we have witnessed several significant achievements with tangible operational results. These included the interagency efforts with the Russia Small Group and Operation Synthetic Theology and also the development and implementation of a strategy that emphasizes continuous engagement, hunting our adversaries forward, and reasserting deterrence in cyberspace.

During this time, we have seen our adversaries adapt, blending cyber and information warfare to form an operational continuum that continues to challenge us in the digital realm. What worked for our cyber forces in helping to secure our 2018 midterm elections will not necessarily guarantee our security moving forward. We must acknowledge the creativity of our adversaries and continue to adapt our playbook. We must ensure that election security is a continuous, sustained effort 365 days a year.

There has been significant progress within the Cyber Mission Force over the past year—specifically, the understanding and categorizing of specific cyber operations forces, the delegation of important operational authorities, the establishment of cyber-peculiar capability development, and the understanding of cyber vulnerabilities within our own installations and weapons systems.

We have made headway to mature our cyber forces, but much work lies ahead. I am interested in hearing what we have learned about the operational needs of the Cyber Mission Force. Are we organized with the appropriate skill sets, number of personnel, and force structure to meet the future needs of the Nation?

As we reevaluate our cyber posture, these findings will be critical to ensuring we align the appropriate resources, policy, and authorities to the Cyber Mission Force to stay ahead of our adversaries and reaffirm the notion of deterrence in cyberspace.

With that, I yield back.

And thank you again to our witnesses.

Mr. LANGEVIN. I thank the ranking member.

Before I recognize Secretary Rapuano, I want to briefly note to our witnesses that the cumulative cyber budget has not been made available to Congress or the American people. The President's budget was formally delivered nearly a month ago, and we are still waiting for the congressionally mandated budget documents for cyberspace operations.

Secretary Rapuano, I am also disheartened that even your opening statement relied only on top-line figures for cyberspace operations. So I hope that the numbers are going to be forwarded to Congress imminently.

With that, I will turn it over to you, Secretary Rapuano. You are now recognized for your opening statement.

**STATEMENT OF KENNETH P. RAPUANO, ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY, AND PRINCIPAL CYBER ADVISOR TO THE SECRETARY OF DEFENSE, U.S. DEPARTMENT OF DEFENSE**

Secretary RAPUANO. Thank you, Chairman Langevin, Ranking Member Stefanik, and members of the committee.

I am pleased to be here today with General Nakasone, Commander of U.S. Cyber Command, to report on the progress that the Department of Defense has made over the past year implementing the 2018 DOD [Department of Defense] Cyber Strategy and working towards the Department's core objectives in cyberspace.

The 2018 DOD Cyber Strategy prioritizes the challenge of great power competition and recognizes that the Department must defend forward to counter our competitors' long-term, coordinated campaigns of malicious activity to gain political, economic, and military advantage.

The strategy normalizes the Department's efforts in the cyberspace domain, integrating cyberspace operations into military operations across all physical domains, and reinforces the need to prevent or degrade threats before they harm U.S. national interests.

Our new approach to competition in cyberspace is enabled by the new Presidential policy on cyberspace operations. Thank you also to Congress for legislation which clarified that cyberspace operations are traditional military activities. Taken together, these changes have advanced the Department's ability to operate in cyberspace, allowing us to execute transparent, well-coordinated, and timely operations.

Since last year, I have been focusing on implementing the DOD Cyber Strategy and effectively closing the gaps identified in the subsequent congressionally directed Cyber Posture Review. To this end, I have augmented the expertise and capacity of the cross-functional team of experts in the Office of the Principal Cyber Advisor.

We have had a number of successes, including: defining the cyber operation forces; initiating the first DOD-wide effort to achieve 100

percent visibility of network devices at the operating system level; defining what constitutes the Department's cyberspace operating force and finalizing readiness standards for the Cyber Mission Force; and, finally, maturing the concept of layered deterrence.

We have also made progress in operationalizing the new, more proactive approach in cyberspace. My guidance from the Secretary is clear: Defending elections is an enduring mission of the Department of Defense. To that end, we are supporting a whole-of-government effort to defend the 2020 elections. The Department, principally through U.S. Cyber Command and NSA's [National Security Agency's] Election Security Group, is complementing other Federal departments by leveraging our unique authorities and capabilities and the proactive approach to defend forward.

Our new, proactive approach in cyberspace is not limited, however, to defending elections. Through outstanding cooperation with the interagency and the NSC [National Security Council], the Department is able to conduct the full range of missions articulated in the NDS [National Defense Strategy] and the DOD Cyber Strategy. Accordingly, our cyber forces are increasingly engaged in cyberspace to promote stability and security and to defend the United States. Our interagency and private-sector partners are key to ensuring that DOD can operate and project power in a contested cyber environment.

The increasingly provocative activities of key competitors demonstrate how vulnerable the Department is to attacks against the many non-DOD-owned assets that are nevertheless critical to our ability to execute our missions. Their vulnerability means that adversaries could disrupt military operations without actually targeting military networks and systems themselves.

To address these challenges, we are strengthening alliances and attracting new partners to take a whole-of-society approach to enabling better security and resilience of key assets.

For example, to enable collaboration and unity of effort between DOD and the Department of Homeland Security in support of protecting critical infrastructure and defense critical assets, we have focused on maturing processes and procedures for cooperation and information-sharing and enabling operational collaboration.

We have taken a range of actions, including carrying out combined training events with DHS [Department of Homeland Security] and private-sector entities and collaborating with DHS to exchange cyber threat information with private-sector entities.

We are also finalizing an agreement with DHS, the Federal lead for improving the security and resilience of much of the Nation's critical infrastructure, to implement section 1650 of the fiscal year 2019 NDAA to allow DOD to provide DHS with up to 50 cybersecurity personnel on a non-reimbursable basis to enhance cybersecurity cooperation and unity of effort.

The key theme of the DOD Cyber Strategy is strengthening international alliances and attracting new partners. In 2019, the Secretary issued new international cybersecurity cooperation guidance to clarify priorities for addressing cyber threats through building the capacities of our international partners and refining responsibilities among DOD components.

The guidance directs how DOD components will collaboratively pursue the objectives of the National Defense Strategy, the National Cyber Strategy, and the DOD Cyber Strategy as they apply to security cooperation in cyberspace.

Thank you for the opportunity to appear before you this afternoon. With the 2018 National and DOD Cyber Strategies in place, we are confident that the Department has the right policy, guidance, authorities, and funding levels to support the defense of our Nation in cyberspace.

I look forward to continue working with you and our critical stakeholders both inside and outside the U.S. Government to build on this process. Thank you.

[The prepared statement of Secretary Rapuano can be found in the Appendix on page 23.]

Mr. LANGEVIN. Thank you, Secretary Rapuano.

General Nakasone, you are now recognized.

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

General NAKASONE. Good afternoon, Chairman Langevin, Ranking Member Stefanik, and distinguished members of the committee. I look forward to discussing the state of U.S. Cyber Command in 2020, its 10-year anniversary from when it was formed.

Today, I want to highlight how Cyber Command is providing clear returns on the investment the Nation has made in it. In the statement I submitted for the record, I explained how Cyber Command is expanding the competitive space for the Department of Defense. Making this all possible are the contributions made by our military and civilian personnel and the support you and the Department of Defense continue to give us.

Let me touch on three issues that are at the forefront of our efforts today: elections, readiness, and the people that make up the DOD cyber force.

We are 244 days from the 2020 Presidential election. My top priority is a safe and secure election that is free from foreign influence.

Our strategy at Cyber Command, working with NSA and other partners across the government, is to generate actionable insights, to harden defenses, and to be ready to impose costs, if necessary. Malicious actors are trying to test our defenses and our resolve. We are ready for them and for any others who may try to interfere with our democratic processes.

I have great confidence in the Cyber Mission Force to execute missions because it is a mission-ready force. Ten years ago, our national leaders envisioned a command that could lead the military's efforts to defend U.S. interests in cyberspace. Today, that vision is a reality.

The Cyber Mission Force is highly trained, well-equipped, and manned by our Nation's finest men and women—Active, Guard, and Reserve military and civilians alike. They provide the Department of Defense and the Nation with capacity to conduct defensive activities, like rapid incident response, and they stand ready to execute a range of cost-imposing operations.

The readiness and operational success of the Cyber Mission Force is a testament to the quality of our people. Recruiting, training, developing, and retaining the best talent is essential for the military to defend the Nation in cyberspace.

I thank you for the legislative flexibility you have afforded the Department to do just that, such as the creation of the Cyber Excepted Service to fast-track civilian hiring. I continue to pursue creative ways to leverage our Nation's best and brightest who want to contribute to our missions, especially through closer partnerships with the National Guard and the Reserves.

Distinguished members of the committee, thank you once again for your support of U.S. Cyber Command. I look forward to your questions.

[The prepared statement of General Nakasone can be found in the Appendix on page 42.]

Mr. LANGEVIN. Thank you, General Nakasone.

We will now go to questions, and I will recognize myself for 5 minutes.

Let me begin—General Nakasone and Mr. Rapuano, in December, the Secretary of Defense signed a memorandum to the Department that created the new term "Cyber Operations Force," which will now encompass the Cyber Mission Force as well as other cyber-specific operational elements.

Can you please help us understand how a definition was decided and which forces were determined to be in the Cyber Operations Force while other operation elements, such as the Air Force's mission defense teams, were excluded?

General NAKASONE. Chairman, as you are well aware, one of the authorities that has been granted to me is the joint force provider role. That is the ability for us at USCYBERCOM and myself, particularly, to have cognizance over select elements of our cyber force DOD-wide.

We initially began with looking at the cyber force as only 133 teams, our Cyber Mission Force. But as we realized, given our three missions, to include securing the Department of Defense Information Network, we needed to have greater visibility over a larger force. So that cyber operational force now is not only 133 teams, but it is also the cybersecurity service providers, the people that run the networks for each of the services.

And I would offer, why is that important? That is important because we want to have the ability to drive training standards that are equal across all of our services. That is a lesson that we have learned with our Cyber Mission Force. One training standard allows us to be interoperable, drives a higher level of training, drives a higher level of capacity.

Mr. LANGEVIN. Can you talk about which teams were excluded and which were not?

General NAKASONE. We looked very carefully, Chairman, at each of the service capabilities. And so those cyber elements that were doing a uniquely service-specific job, such as a defensive job for unique weapon systems, we looked at that and we thought that that was a service retain mission and one that would remain in the cognizance of the services.

Mr. LANGEVIN. So how many people will be part of the new Cyber Operations Force?

General NAKASONE. Roughly, back-of-the-envelope math, Chairman, I would say the 6,187 that are part of our Cyber Mission Force. And then I would say probably double that with regards to our cybersecurity service providers across all four services.

Mr. LANGEVIN. Okay. All right. Thank you.

So my next question. Cyber Command right now is being utilized today to a greater degree than ever before. For all the various mission sets and the demand signal from the Secretary and the other combatant commanders, do you believe that the approximately 6,100 personnel in the Cyber Mission Force is the right size? And if not, what would be the correct size?

General NAKASONE. Chairman, as you know, we created the Cyber Mission Force in late 2012 and started building it in 2013. It was designed on 133 teams, given the planning that we had at the time.

What has changed since 2013? We are starting now to do election support, an enduring mission, as our Secretary has talked about. We have seen our adversaries have gone from exploitation, disruption, destruction into influence operations. We see the defend-forward strategy that our department has now, what we at U.S. Cyber Command are doing as persistent engagement, and we see the corresponding hunt-forward missions. Finally, we see across our services the necessity not just to defend networks but also to be very careful in defending our data and our weapons systems as well.

That is a long response to say what we are doing, given all of those missions, is, through a series of exercises this year, looking to gather data; what is the right size force that we need? Obviously, as a commander, I would tell you that I never have enough forces, but what I do need is I need the ability to show that in data.

And when we come back to that, we will provide that, obviously, to the Department. And the Department, through their process, will make a determination on the right size force.

Mr. LANGEVIN. Okay. And can you talk about the zero-based review in the 2020 NDAA and how it will address any existing deficiencies?

And, also, how quickly are the services prepared to grow the pipeline needed to provide you with the force to fill out the deficiencies between your current strength and your ideal size?

Secretary RAPUANO. I would note that we had an exercise not long ago with the Secretary of Defense with the NDS Implementation Group looking at cyber and went through the whole framework. General Nakasone did an outstanding job briefing.

But the issue of our force sizing came up. And there was a lot of emphasis—just as General Nakasone has just explained, this was at the very beginning; 2013 versus 2020 is a whole new paradigm in terms of the evolving threat and in terms of our evolving understanding of the needs.

So the Secretary directed at the end of that meeting that we conduct this assessment, which will be supporting the response to the NDAA requirement.

Mr. LANGEVIN. Okay. Thank you.

The ranking member is now recognized for 5 minutes.

Ms. STEFANIK. I am going to yield my time to Rep. Gallagher.

Mr. GALLAGHER. Thank you.

And thank you to both of you gentlemen for your active participation in the Cyber Solarium Commission; General Nakasone, for making yourself available on numerous occasions to brief the Commission; and Mr. Rapuano, for being an active member of the Commission and having an almost perfect attendance record on the Commission's meetings, which I know is hard to achieve. And most Members of Congress on the Commission did not even achieve that attendance record.

So we are really looking forward to unveiling the final report, which would not have been possible were it not for the leadership of Chairman Langevin and his active engagement in it. So we hope it is a start of a very robust discussion about not only how far we have come under both of your leadership but how far we still need to go and where we can improve.

And just to kind of follow up on the line of questioning from the chairman, just to put a point on it, General Nakasone, since the Cyber Mission Force was created, it is fair to say the demands on that force have increased.

So, while we can't say here today that you need to increase the Cyber Mission Force by X number and it is going to cost this amount of dollars, it would be fair to say, if we were to do a force structure assessment of the Cyber Mission Force, it would probably come back with an expanded vision for the Cyber Mission Force, correct?

General NAKASONE. So, Congressman, I would offer that, I think as we take a look at the expansion missions, that obviously there will likely be, you know, a corresponding look at what the proper size needs to be.

If I might, one of the things that I perhaps didn't emphasize enough that I think really has changed tremendously is the fact that the strategies, the policies, the authorities have all changed dramatically even in the past 24 months. And that has driven a larger OPTEMPO [operational tempo], an OPTEMPO we can talk about in closed session today. Because I think you can see, given the right strategy, policies, and authorities, what this force is able to do.

Mr. GALLAGHER. And then just to the extent you can, give us a sense of what your team was doing last night in near-real-time as you have tried to, kind of, learn the lessons of 2016. Just give us a taste of what that looks like.

General NAKASONE. So, Super Tuesday, yesterday, team comes in at 6 o'clock in the morning. We have teams ready to go. We have the interagency up on one chat system, so we are talking between the Department of Defense, Department of Homeland Security, intelligence community. We have a very good feel from elements of our National Guard in certain States of what is ongoing.

This is all different than what we were doing in 2018. In 2018, I look back on that, even though very successful, it looks like a pickup game to me, as opposed to what I saw yesterday—constant communications. "Hey, we see indications of a problem here." "Do

we see any indications in foreign intelligence that that might be indicative of someone making a move?" "No, we don't."

This is the type of interaction—rapid. I think it is representative of the domain in which we operate, but I think it is also the idea of we have all of these elements together. The National Security Council is online. We have a really good sense of, across the interagency and across the whole of government, how we operate.

Ms. STEFANIK. Reclaiming my time, I am going to yield to Mr. Waltz to give other members an opportunity.

Mr. WALTZ. Thank you.

Just continuing on the election security piece, over 9,000 counties across the United States, different operating systems, different levels of talent, different funding.

How do we—number one, I think it is worth noting that the Guard is the only entity that is in all 9,000 counties across the United States. So, question one, what more can the Guard do, from an election security piece?

Number two, are we thinking about this in the right way, in the sense of deterrence, right? Can we possibly bat 1,000? Can we possibly defend perfectly? Or, if we have a foreign adversary attacking what we have labeled critical infrastructure, do we need more of a deterrence posture? And what would that look like?

General NAKASONE. Congressman, if I might begin with what our strategy is in Election Security Group, because I think this is a part of the answer to your question.

So what are we doing? We are really operating under three focus efforts right now. One, how do we generate maximum amount of insights on our adversaries? We want to know our adversaries better than they know themselves.

Secondly, how do we improve the defense? How do we work with the Department of Homeland Security to ensure election infrastructure is more readily defended? And how do we work closely with the FBI [Federal Bureau of Investigation] to provide information to social media companies to ensure that they have it?

And then, thirdly, how do we impose cost?

I would offer, one of the things that has been to our advantage is we have the experience of 2018, but the other thing is that we are not approaching this episodically. Since the 8th of November in 2018, we have been working this issue, and we are continuing to look at how do we continue to engage with our adversaries in a number of different means to ensure that they understand that we see what they are doing.

Mr. WALTZ. I just—I know we are out of time. I think you are doing a fantastic job. Things are far better than they were in 2016. But I think we need to make it clear that this is only going to stop when the other side understands that we have the capability and will to impose costs on their system. And that is a sea change. It is kind of like going from counterterrorism in the 1990s to post-9/11 in terms of how we are thinking about it.

And I yield my time. Thank you, Ranking Member.

Ms. STEFANIK. I yield back.

Mr. LANGEVIN. The gentleman's time has expired.

Mr. Larsen is now recognized.

Mr. LARSEN. Thank you, Mr. Chairman.

General Nakasone, along those same lines, we talked a little bit about this yesterday, but I have had eight townhalls since the beginning of the year in my district. And every townhall has its own set of issues. You are in a local area, they bring up local issues, and so on. But I will say, every townhall I have had, two sets of questions come up. One of them is on election security and what are we doing to be ready for 2020.

So the question I asked yesterday, and I was wondering if you could just cover that, is: Given the fact that some of what we are doing we can't talk about publicly, you know, how do we talk about, how do we communicate to the average citizen who wants to know that the United States is doing its dead level best? What are the actions that we are taking and what can we describe to folks about the actions we are taking to ensure the integrity of the vote?

General NAKASONE. Congressman, regarding that question, I think the discussion point of what we are discussing today is so important. So what is the Department of Defense doing to ensure a safe and secure election?

First of all, putting our assets, to include our finest intelligence from the National Security Agency, operating outside the United States, to understand what a variety of adversaries might want to do.

Secondly, working across the government, so the Department of Defense working across the government with DHS, with the intelligence community, with other elements, to share intelligence—I mean, to share insights to improve our defenses, both at the State and local level for DHS as they work with the State and local level; also with the FBI, where they are working with the platform owners of, you know, social media platforms that are being utilized by our adversaries often to message our population.

And the third thing is a range of actions that we are operating today—and we can get into more detail in closed session—to impose costs on our adversary. Any adversary that intends to interfere with our democratic process should know that we are going to take action. We have the authorities, we have the policy, we have the strategy, we have the will. And we demonstrated that will in 2018.

Mr. LARSEN. This might be for both of you. A lot of focus, obviously, on election security in the subcommittee today. With all that you are learning and relearning and putting in the feedback loop to learn some more about election security, how else are we using these young women and men who are in Cyber Command?

Are we creating an expertise in election security as well as making sure they have the expertise in supporting combatant commanders for other things? Are we starting to create divisions—not divisions in a bad way, but sub-agencies within Cyber Command? Do we have expertise? How are you approaching that?

General NAKASONE. When we stood up our Cyber Mission Forces, we had three missions that they were dedicated to, as you will recall: One was defend our networks, two was to support combatant commanders, and the third piece is to defend our Nation in cyberspace.

Primarily, we are using the element which is the Cyber National Mission Force, a unit I know very well, I commanded previously,

as the action arm for defending the Nation in cyberspace with regards to elections.

I don't think it overly specializes them. In fact, what I would tell you is we are seeing influence operations across a spectrum of different actors. And so being able to understand this, being able to work an election is pretty important for us.

Mr. LARSEN. Okay.

Secretary RAPUANO. I would just add to that and the point that General Nakasone made earlier, this truly is a whole-of-government and even a whole-of-society exercise.

And one of the greatest shifts that we have seen over time, even in the last year, is the whole-of-government enterprise has matured dramatically. First, you have a much better appreciation for the threat. The perception of the threat is much more palpable today than I think it has ever been before.

Secondly, you have seen agencies and departments really up their game. You can look at the Department of Homeland Security and CISA [Cybersecurity and Infrastructure Security Agency]. You can look at other elements of the DHS, but the FBI and Justice Department. They bring unique authorities and capabilities, and they have added significantly.

So it is not about Cyber Command now doing things that aren't military missions. They are using their military skill sets, and they are focused on defending forward, getting at the source of the insult. And they are supporting, through intelligence and warning and in some cases defense support to civil authorities, those civil agencies requesting support. So it gets back to that rapid maturation loop that we have seen in just one year.

Mr. LARSEN. Yeah.

Secretary RAPUANO. Thank you. Or 2 years, sorry.

Mr. LARSEN. Two years, yeah. Thank you.

And I yield back. Thank you.

Mr. LANGEVIN. Thank you, Mr. Larsen.

Mr. Conaway is recognized.

Mr. CONAWAY. No questions.

Ms. STEFANIK. Can you yield to Bacon, please?

Mr. CONAWAY. I yield to Bacon.

Mr. LANGEVIN. Mr. Bacon is recognized.

Mr. BACON. Thank you.

Thank you to both. Appreciate you being here.

I have a related question on the war powers resolution coming up. It was voted out of the Senate. It implies that we are doing continuing operations against Iran, which I dispute. We did a one-time kinetic operation against General Soleimani, who was in Iraq doing war planning, someone who killed 609 Americans.

But here is my concern. So this will limit kinetic operations, but I think it also—it doesn't just say "kinetic." It implies any military operations. And what I wonder about, what is the impact on Cyber Command if this war powers resolution passes both Houses and becomes law?

Secretary RAPUANO. I don't see it impacting Cyber Command at all, but I will turn to General Nakasone.

General NAKASONE. I don't either, Congressman. I see us continuing to operate below the level of armed conflict. I have all the authorities and the policies that I need to continue to operate.

Mr. BACON. Thank you.

Secondly, there are two articles that talked about our successful operations in the 2018 election, but I don't think the voters really know much about it. What can you say as to your success in the 2018 election to foil what the Russians were doing?

Secretary RAPUANO. I think we can say a lot more in a closed hearing, but, again, I will turn to ——

Mr. BACON. And whatever you can publicly say. I think it is helpful for our citizens to know, though, to the best extent that we can. Because this is a success, and it is not really well known.

Secretary RAPUANO. So, Congressman, while I won't speak to the articles, what I will speak to is the fact that, what was different in 2018.

What was different in 2018 is, again, we had the strategy, policies, and authorities that we needed to carry out our missions against an adversary that was attempting to influence our population.

Secondly, we had the will to act, the will from policy makers and certainly all the way down, and we acted.

And the third thing is that we have a very, very highly trained force that is very, very capable.

Mr. BACON. Thank you.

A third question. When I came in 3 years ago, there was a discussion of trying to dual-hat—or not dual-hat—put two different four-stars, one for NSA, one for Cyber [Command].

I thought it was a mistake because I know our teams are combined, NSA and Cyber, particularly for cyberattack. It is definitely a synergistic team there. I think it works well to have a single four-star with two different three-stars.

But is there any more discussions on separating with two different four-stars, or is this the organizational construct for the long term, which I hope it is?

Secretary RAPUANO. Any decision on the dual-hat arrangement and changes to the dual-hat arrangement would really be the considered judgment collectively of the Secretary of Defense, the Chairman of the Joint Chiefs, and the Director of National Intelligence.

So that certainly is a possibility, but right now that is not a focus in terms of what leadership is looking at with regard to our cyber activities.

Mr. BACON. Okay. I hope it is not, because I think it is useful to have a common direction for both the Cyber side and the NSA side on these teams, and having a single four-star provides that unified effort. To have two different four-stars, it could work. It is personality-dependent. But I also think it is a recipe for disaster. So I think we have the right construct now.

We have 6,100 people that are serving in the Cyber Mission Force. Is that the right size? Is this working?

General NAKASONE. So certainly it is working. I think whether or not it is the right size for the future, that is part of the issue that we are going to take on this year through a series of different

exercises to get the data to take a look at what is the right size force given the missions and the requirements from the Department.

Mr. BACON. One final question, because I have about a minute and a half left. Obviously, I am interested in this entire topic. I think you guys do great work.

You know, in the Air Force, they combine their cyber and EW [electronic warfare] into a common command under Air Combat Command. But at the combatant command level, we have cyber under yourself, sir, and then we have also EW under STRATCOM [U.S. Strategic Command].

Is this organization division, is it working, or do we need to relook at that?

General NAKASONE. Let me address 16th Air Force first, because I am a huge fan of what General Goldfein has done, bringing together AFCYBER [Air Force Cyber Command], which was the 24th Air Force, along with the 25th. Under one commander, 10 wings, able to do cyber, IO [information operations], EW, intel.

Why is that important? Because, rapidly, the commander of 16th Air Force, AFCYBER, can move with a number of different opportunities to get at adversaries. And what I just listed there are all non-kinetic means that have tremendous capabilities against our adversaries.

So my hat is off to the Air Force.

Mr. BACON. You don't see any need to make any changes with the EW/cyber at the combatant level?

General NAKASONE. Well, again, I think this is something the Joint Staff will continue to study.

Mr. BACON. Okay.

General NAKASONE. We are a learning organization. We are a work in progress. And I think that, as we continue to mature, it will probably take a look at what is the right laydown of all the non-kinetic elements.

Mr. BACON. Right. I personally don't have a position. I was just curious for yours, so I thank you.

Secretary RAPUANO. There are a lot of trades, obviously. And the more time that we have in the hole, in terms of operating in each of these areas, particularly the new warfighting domains—cyber, space—we are going to develop a better appreciation for where the synergies are and, as importantly, where the organizational strengths are in terms of what our structure and business process is.

Mr. BACON. Okay. Mr. Chairman, I yield back.

And thank you to both these great leaders.

Mr. LANGEVIN. Thank you, Mr. Bacon.

Mr. Brown is now recognized.

Mr. BROWN. Thank you, Mr. Chairman.

I have some really basic questions. I will field both of them. Take the time that you have to devote to it however you want.

Army, a new accession officer into cyber, can you tell me about how you bring that officer in, what kind of training they go through, the assignments they need to be an effective, let's say, O–6 in the Cyber Command?

And then the second question I have is, can you assess publicly—and I know that there have been some reports recently about, sort of, like, your storage capacity, your ability to exploit data, to capture adversary information and analyze it. Can you talk about the infrastructure you have and give me an assessment, whether you have what you need? Because you take in a lot of information every day, and do you have what you need to evaluate it, exploit it, act on it, et cetera?

General NAKASONE. Congressman, the question that you ask is one that I have a tremendous amount of interest in, because our number one priority at U.S. Cyber Command is our people. And let me talk a little bit about accessions, particularly for our Army, because I know that best.

So two major places you are going to come if you are a cyber officer, either from United States Military Academy or ROTC [Reserve Officer Training Corps]. I believe that cyber is the top, if not close to the top, requested branch across Army in new lieutenants coming in. This is a popular branch that very, very talented people want to get into.

We accept about 120 a year, if I am not mistaken. And from that, your initial assignment is going to be at Fort Gordon, Georgia, for basic officer leadership course, where you have both the technical, the tactical, the leadership abilities that are going to be trained as you serve there.

First assignment likely in one of four places: Fort Meade, Maryland; Fort Gordon, Georgia; Texas; or Hawaii. You are likely going to be leading one of our offensive or defensive teams. So a very similar leadership construct that you are obviously very familiar with, but it also builds in terms of, as you get more proficient, as you are able to show your technical prowess, as you are able to lead soldiers, then greater responsibilities would occur.

In terms of the data, we have, through your strong support in the committee here, a Joint Cyber Warfighting Architecture that is being funded right now.

One of the key elements of that is increasing our data. It is called the Unified Platform. That is now starting to come online and, over the next year, will be really the central focus in terms of building this warfighting architecture that allows us to store data and then be able to conduct operations worldwide.

Mr. BROWN. Thank you.

I yield back, Mr. Chairman.

Mr. LANGEVIN. Thank you, Mr. Brown.

We are going to have to recess here. We have two votes, and then we will come back for the closed session. I know Mrs. Trahan had a question she wanted to ask in closed session.

So, at this point, then, unless there are any further questions—Ms. Stefanik, do you have any more questions?

Ms. STEFANIK. No questions.

Mr. LANGEVIN. We will adjourn, and we will come back to closed.

[Whereupon, at 4:10 p.m., the subcommittee proceeded in closed session.]

# A P P E N D I X

MARCH 4, 2020

**PREPARED STATEMENTS SUBMITTED FOR THE RECORD**

MARCH 4, 2020

**Opening Statement**
**Chairman James R. Langevin**
**Intelligence and Emerging Threats and Capabilities Subcommittee**

**FY 2021 Budget Request for Military Operations in Cyberspace**

**March 4, 2020**

The subcommittee will come to order. Welcome to today's hearing on the Fiscal Year 2021 Budget Request for Military Operations in Cyberspace.

I'd like to welcome our witnesses.

Mr. Kenneth Rapuano serves as both the Assistant Secretary of Defense for Homeland Defense and Global Security and as the Principal Cyber Advisor to the Secretary of Defense. Prior to returning to government service, Mr. Rapuano worked for Federally Funded Research and Development Corporations, focusing on homeland security and counterterrorism issues. Mr. Rapuano, welcome back.

General Paul Nakasone serves in three capacities concurrently: Commander of U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Service. Before his current role, he commanded U.S. Army Cyber Command, and has served as a career intelligence officer through his 33 years in uniform. General Nakasone, thank you for your extraordinary service to the Nation. We are pleased to have you back here with us today.

The Department of Defense created U.S. Cyber Command (CYBERCOM) in 2009, and more than ten years later, we are still working diligently on establishing the foundations, concepts, doctrine, training, and metrics needed to ensure the security of the nation in the cyberspace domain.

The state of cyber in national defense is more central than ever, and 2020 marks a sea change, with cyber firmly established and accepted as a warfighting domain, capability, and asset. This is highlighted best through the current operational posture and institutional maturation of CYBERCOM.

Over the course of 2020, this subcommittee expects the Command to aggressively address issues of readiness, operational tempo, and the defense of the nation's electoral system. This Committee has worked to ensure that the Department, the military services, and CYBERCOM are equipped with the tools and authorities necessary to achieve their objectives. In the FY2020 NDAA, we granted new authorities to CYBERCOM, and bolstered multiple frameworks for legislative oversight. We seek to balance an appropriate degree of oversight while ensuring the command retains operational flexibility. We will continue this trend through our collective work in the FY 2021 bill.

CYBERCOM is facing possibly the most challenging year in its existence. General Nakasone, your command sits at the center of the Department's efforts to secure the information environment.

The United States faces increasing malicious cyberactivity from Russia, Iran, China, and others. We know about how Russia weaponized information

during the 2016 election, and we must do more to anticipate and counter these sophisticated operations. While we have had some success countering Russia's malign influence campaigns in 2018, we must not let our guard down. We must ensure that we are properly organized within the Department of Defense and coordinating across the US Government. I hope you will give us a full assessment of your efforts to protect the country from malign cyber activity. I will be particularly interested to hear how you are working with partners in the interagency to promote a more stable cyberspace and protect our – and our allies' - critical infrastructure. I will want to hear specifically how your are coordinating and deconflicting activities domestically with the Department of Homeland Security and internationally with the Department of State.

I am also interested to hear from our witnesses about their assessment of CYBERCOM's current force structure. For the past year, I have had the privilege of serving on the Cyberspace Solarium Commission – and I thank you, Mr. Rapuano, for your many contributions to our work. One of the areas of focus of the commission has been whether CYBERCOM's force structure properly reflects the Command's operational aspirations. Essentially, we need to candidly assess whether a force conceived more than seven years ago is sufficient for a dramatically different environment today. I will also be curious to hear candid assessments on how organic capabilities resident in the Services are rationalized with CYBERCOM's mission and strategy.

Throughout our nation's history, our military has grown accustomed to focusing on the offensive systems, forces, and platforms that deliver effects against our adversaries. Given our geographic advantage of two oceans, and our history of primarily fighting overseas, we are conditioned to fight offensively. However, in a connected world, with an inestimable number of internet-connected devices, networks, vehicles, and systems, our defensive posture in the cyber domain has never been more critical.

While I fully support CYBERCOM's more offensively postured construct, I am concerned that the President's FY 2021 cyber budget signals in select places that we can sacrifice defensive programs and investments in favor of investments in offensive cyber systems and programs. I hope the witnesses will speak candidly about balancing resources to ensure the Department is best postured to protect the United States in cyberspace, whether through defensive or offensive missions.

With that, I want to thank our witnesses for appearing before us today. As a reminder, after this open session, we will move to room 2337 for a closed member-only session.

I'll now turn to Ranking Member Stefanik for her remarks.

STATEMENT OF

MR. KENNETH RAPUANO

ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND

GLOBAL SECURITY

AND PRINCIPAL CYBER ADVISOR

TESTIMONY BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND

CAPABILITIES

MARCH 4, 2020

Thank you Chairman Langevin, Ranking Member Stefanik, and Members of the Committee. I am pleased to be here with General Nakasone, Commander of U.S. Cyber Command (USCYBERCOM), to report on the progress the Department of Defense (DoD) has made implementing the 2018 DoD Cyber Strategy and achieving the Department's objectives in cyberspace. This afternoon, I am testifying in both my roles as Assistant Secretary of Defense for Homeland Defense and Global Security, and as Principal Cyber Advisor (PCA) to the Secretary of Defense. I am responsible for advising the Secretary and the Deputy Secretary on cyberspace activities and the development and implementation of the Department's cyber strategy and cyberspace policy; leading our interagency partnerships and coordination of our whole-of-government cyber efforts; engaging with our allies and partners; and ensuring the integration of cyber capabilities across the Joint Force in support of the President and Secretary of Defense.

**Strategic Context**

To start, I would like to offer our perspective on the current threat environment. As our National Defense Strategy (NDS) makes clear, we are in a renewed era of great power competition. Strategic competitors such as Russia and China are asserting their military and non-military power to challenge the rules-based international order. Although our military superiority has deterred conventional aggression against the United States, states such as China, Russia,

North Korea, and Iran are increasingly taking actions in the gray zone below the threshold of the use of force to undermine our security. There is perhaps no area where this is more true than in cyberspace.

For more than a decade, our competitors have taken actions in and through cyberspace to harm the United States, our allies and partners, and the international order. Our competitors are conducting long-term, coordinated campaigns of malicious activity to gain political, economic, information, and military advantage. Their objective is to "win without war," and, in the event of a conflict, to leverage accesses and capabilities developed prior to hostilities to achieve decisive military advantage.

The Intelligence Community (IC) assesses that China, Russia, Iran, and North Korea are using, and will continue to use, cyber capabilities to steal information, to influence our citizens, to undermine democratic institutions, and to prepare to disrupt critical infrastructure that our national security depends on.

China remains a persistent and growing threat to the United States in cyberspace. As Secretary Esper said at the Munich Security Conference in February 2020, China is seeking to gain an advantage over the United States by any means, at any cost, including by exerting its growing power in ways that are threatening, coercive, and counter to the rules-based international order. China's

growth has been fueled by theft, coercion, and the exploitation of free market economies, private companies, and academia. These activities are enabled by China's cyber capabilities, as we saw from the Justice Department's (DOJ's) recent indictment of four members of the PLA for hacking Equifax to steal valuable trade secrets and the personal data of Americans. The IC also assesses that China maintains the ability to use its cyber capabilities to cause localized, temporary, and disruptive effects on critical infrastructure inside the United States.

Russia continues to be a highly sophisticated and capable adversary, integrating cyber espionage, attack, and influence operations in mutually reinforcing ways to achieve political, economic, and military objectives. The IC assesses that Russia is pre-posturing capabilities that could disrupt or damage U.S. civilian and military infrastructure before or during a crisis. We have already seen Russia conduct such attacks against our allies and partners, including the October 28, 2019, attack against the Republic of Georgia that disrupted thousands of websites and at least two major television stations.

Although China and Russia remain our two primary strategic competitors, the threats to the United States in cyberspace include a diverse set of additional actors. Iran and North Korea are employing their cyber capabilities to conduct espionage, and they remain a threat to public and private U.S. critical infrastructure. Terrorists and violent extremists continue to leverage the digital

domain to advance their agenda. And the growing availability and use of publicly and commercially available cyber tools is increasing the overall volume of unattributed cyber activity around the world.

The digital domain also enables campaigns of malicious foreign influence with the goal of shaping our alliances and partnerships, policy outcomes, and, most significantly, undermining our democratic institutions. As you have frequently heard from our IC colleagues, threats to U.S. elections this year could be broader and more diverse than before, as more nations and other actors attempt to interfere with U.S. institutions and society by targeting social media and elections infrastructure.

It is in this context of determined, rapidly maturing adversaries that the 2018 DoD Cyber Strategy called for a more proactive approach to competing in the domain. We can no longer allow our strategic competitors to flout norms of responsible state behavior in cyberspace while claiming to be responsible actors. The DoD Cyber Strategy normalizes the Department's activities in cyberspace by directing the Joint Force to integrate cyber operations fully into military operations. The Cyber Strategy also makes clear that the Department's focus in cyberspace, like in other domains, is to prevent or mitigate threats before they harm U.S. national interests. The Department will "defend forward" in cyberspace

in the same way we operate outside our borders on land, in the air, at sea, and in space to understand and defeat threats before they reach the United States.

The Department defends forward by conducting operations that range from collecting information about hostile cyber actors, to exposing malicious cyber activities and associated infrastructure publicly, to directly disrupting malicious cyber actors. In order to be successful, we must be in malicious cyber actors' networks and systems and continually refresh our accesses, capabilities, and intelligence. Defending forward simultaneously puts "sand in the gears" of the offensive operations of malicious cyber actors, and generates the insights that enable our interagency, industry, and international partners to strengthen their resilience, address vulnerabilities, and defend critical networks and systems.

Finally, cyber – unlike many other domains – is a field where people are the real capability. As the first inaugural President's Cup Cybersecurity Competition proved, the nation's best cyber defenders are in uniform. I took particular note of the fact that out of thousands of competitors, our nation's best individual cyber professional is a Cadet First Class at the Air Force Academy. The Department remains committed to using the authorities granted to it by Congress – including new pays, promotions, and commissioning tools – to grow an experienced cyber cadre of talented professionals capable of tackling the world's hardest digital tasks.

The Department values its partnership with Congress, which has ensured that we have the authorities and policies in place governing cyberspace operations to enable our strategic approach to compete and prevail in the cyber domain. This includes, as provided in the National Defense Authorization Act for Fiscal Year 2019 (NDAA for FY 2019), both the affirmation of the President's authority to counter active, systemic, and ongoing campaigns in cyberspace by our adversaries against the Government and the people of the United States (Section 1642) and the clarification that certain cyber operations and activities are traditional military activities (Section 1632).

**Implementation of the DoD Cyber Strategy: Overview of Progress To-date**

The DoD Cyber Strategy set out five core objectives for the Department in cyberspace. These objectives are: (1) Ensuring that the Joint Force can achieve its missions in a contested cyberspace environment; (2) Strengthening the Joint Force by conducting cyberspace operations that enhance U.S. military advantages; (3) Defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident; (4) Securing DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks; and (5) Expanding DoD cyber cooperation with interagency, industry, and international partners.

We have taken major strides toward being able to achieve these objectives. However, much work remains ahead of us. In particular, we have devoted substantial attention to three areas.

First, we are maturing the nine lines of effort identified in the strategy. These lines of effort include objectives such as: empowering timely, integrated cyberspace operations; modernizing networks and systems; protecting the Defense Industrial Base (DIB); enabling allies and partners; workforce development; and deterrence and mission assurance. Achieving these objectives requires a Department-wide effort to translate relatively broad strategic guidance into specific objectives, tasks, and subtasks that are focused on outcomes. Integral to this effort is the ability to measure results clearly and objectively so that we can assess outcomes. We are not only refining end-states, but also developing project plans, tasks, and measures of effectiveness and performance so that we can continually monitor and evaluate our progress.

Second, we are directing funds to priority areas to address critical gaps identified in the congressionally directed Cyber Posture Review. For example, the FY 2021 budget request includes increased resources for modernizing networks and systems through investments in cross-domain solutions, next-generation encryption development and deployment, and network modernization technologies, such as "Comply to Connect" and "Automated Continuous Endpoint Monitoring."

Third, we have focused on building and employing a cross-functional team of experts, in the Office of the Principal Cyber Advisor (OPCA), to manage actively the implementation of the process across the entire DoD enterprise. The Department has augmented the expertise and capacity of OPCA, allowing closer collaboration with Principal Staff Assistants on key issues, and enabling assessment to inform and advocate for DoD Cyber Strategy implementation throughout the Department.

Although we still have a long way to go, the Department's focused effort on strategy implementation has delivered some important achievements in the past year. Some quick highlights include:

- Initiating the first DoD-wide effort to achieve enterprise-wide visibility at the operating system level and to enable automated federating reporting using common software tools. The standardized use of this tool across the enterprise allows Joint Forces Headquarters Department of Defense Information Network (JFHQ-DoDIN) to visualize and defend the network more effectively.
- Defining what constitutes the Department's Cyberspace Operating Force and finalizing readiness standards for the Cyber Mission Force that will allow the Department to measure readiness accurately across the Services.

- Working closely with other U.S. departments and agencies and the Cyberspace Solarium Commission to mature the concept of layered deterrence. Layered cyber deterrence combines traditional deterrence mechanisms and extends them beyond the Federal Government to develop a whole-of-society approach. It also incorporates the concept of defending forward to address the range of malicious cyber activity that the United States has thus far been unable to deter.

**Putting Our New Cyberspace Authorities Into Practice**

Our new, proactive approach to competition in cyberspace is enabled by new Presidential policy on cyberspace operations, as well as by legislation, including the NDAA for FY 2019, which complements and strengthens the Department's authorities. Taken together, these changes have advanced and modernized the Department's ability to operate in cyberspace, resulting in transparent, well-coordinated, timely operations.

These new policies and authorities have been instrumental in enabling the Department's efforts in support of protecting the integrity of U.S. elections, both in 2020 and looking to the future. My guidance from the Secretary is clear: defending U.S. elections is an enduring mission of the Department of Defense. To that end, we are supporting a whole-of-government effort to defend the 2020 U.S. elections. The Department, principally through U.S. Cyber Command's and

NSA's Election Security Group, is complementing the work of other Federal departments and agencies by leveraging DoD's unique capabilities and capacity and our proactive approach to defend forward. We are countering interference and covert foreign influence against our elections by:

(1) Generating insights to understand adversary activity;

(2) Enabling domestic partner departments and agencies, for example, by sharing indications and warning of indicators of compromise or threat activity with the Department of Homeland Security (DHS) to help them better protect our systems and providing information to the FBI to help expose covert influence online; and

(3) Conducting cyber operations to disrupt, degrade, or defeat malicious cyber activity.

The November 5, 2019, Joint Statement on Ensuring Security of the 2020 Elections released by the Attorney General, Secretary of Defense, Acting Secretary of Homeland Security, Acting Director of National Intelligence, and others, highlights the threat to our elections posed by Russia, China, and Iran. The expansion of the Department's cyberspace authorities is a recognition of the changing cyber threat landscape and the need to position DoD to support whole-of-government efforts by enabling a more proactive and assertive approach during day-to-day competition to deter, disrupt, and defeat foreign cyber campaigns. The

Department, through USCYBERCOM, the National Security Agency (NSA), U.S. Indo-Pacific Command, U.S. Northern Command, and the National Guard Bureau, is poised to support and complement the efforts of DHS and FBI in protecting U.S. elections.

Defending Forward in cyberspace is not limited, however, to defending U.S. elections. Through outstanding cooperation with our interagency partners and the National Security Council staff, the Department is able to conduct the full range of missions articulated in the NDS and DoD Cyber Strategy. Accordingly, our cyber forces are increasingly engaged in cyberspace to promote stability and security and to defend the United States.

Empowered with the necessary authorities, a new strategy, and increasingly close collaboration with our interagency and international partners, we are developing innovative concepts of operation. For example, the Cyber National Mission Force executes "hunt forward" operations involving the deployment of defensive cyber teams globally at the invitation of allies and partners to look for malicious cyber activity. Upon discovering malicious software, one option Cyber Command has employed successfully is to publicly expose malicious signatures to the cybersecurity community, allowing organizations and individuals around the world to mitigate identified vulnerabilities, thereby degrading the efficacy of malicious tools and campaigns.

**Progress of DoD Partnerships Across the Federal Government and With the Private Sector**

Our interagency, international, and private sector partners are key to ensuring that the Department can achieve its objectives in cyberspace. The increasingly provocative activities of key competitors, such as the NotPetya cyber operation conducted by Russia in February 2018, demonstrate how vulnerable the Department is to attacks against the many non-DoD-owned assets that are nevertheless critical to our ability to execute our missions. These assets include civilian ports, airfields, energy systems, and other critical infrastructure. Vulnerabilities in these areas will likely be targeted by our adversaries to disrupt military command and control, financial operations, the functioning of operationally critical contractors, logistics operations, and military power projection, all without ever targeting the comparatively well-protected DoD Information Network. Any large-scale disruption or degradation of national critical infrastructure represents a significant national security threat.

To address these challenges, the DoD Cyber Strategy directs DoD to strengthen alliances and attract new partners to ensure that we are taking a whole-of-society approach and to enable better security and resilience of key assets. In the past year, we have made some notable progress to enable DoD missions through both domestic and international partnerships.

For example, to enable collaboration and unity of effort between DoD and DHS concerning critical infrastructure and defense-critical assets, we have focused on maturing processes and procedures for cooperation and information sharing and for enabling operational collaboration. Under this framework, which stemmed from a 2018 Secretary of Defense-Secretary of Homeland Security memorandum, DoD:

- Established an Executive Steering Group (ESG) to coordinate DoD-DHS collaboration for the protection of critical infrastructure from cyber threats;
- Carried out combined public-private training events with DHS and private sector entities to enable DoD cyber forces to understand more fully the domestic critical infrastructure that they may be called upon to defend;
- Collaborated with DHS to exchange cyber threat information with private sector entities to enable the Department to understand more fully adversary cyber tactics, techniques, and procedures;
- Exercised with DHS to refine our respective roles and procedures during a cyber incident; and
- Conducted combined planning to ensure that, if DHS requests DoD support in a crisis, DoD cyber forces would be prepared to augment DHS's cyber incident response elements.

Additionally, we are finalizing a Memorandum of Agreement between DHS and DoD to implement Section 1650 of the NDAA for FY 2019, which authorizes DoD to provide DHS with as many as 50 cybersecurity technical personnel, on a non-reimbursable basis, to enhance cybersecurity cooperation, collaboration, and unity-of-government efforts. This enhanced collaboration under Section 1650 is an example of what can be achieved when the Legislative and Executive Branches make common cause.

Although individually none of these engagements itself represents a strategic change to the Nation's posture in cyberspace, they together reflect a new pattern of systematic collaboration and engagement among DoD, DHS, and our critical infrastructure partners. Such engagements, sustained over time, are helping to build a united approach that strengthens our national ability to prevent, respond to, and mitigate complex cyber threats.

With international partners, DoD is driving new approaches to expand and strengthen traditional security cooperation tools in support of these important relationships. In 2019, the Secretary of Defense issued new International Cyberspace Security Cooperation Guidance to clarify priorities for addressing cyberspace threats through building the capacities of our international partners and refining responsibilities among DoD components. The guidance directs how DoD components will collaboratively pursue the objectives of the National Defense

Strategy, the National Cyber Strategy, and the DoD Cyber Strategy, as they apply to security cooperation in cyberspace.

In parallel with development of the new Security Cooperation Guidance, DoD has been leveraging 10 U.S. Code Section 333 Building Partner Capacity resources in advancing security cooperation in the cyber domain with our international partners. It is our aim over the coming year, in furtherance of the DoD Cyber Strategy and with the continuing support of Congress, to build on our existing cyber-related capacity-building engagements overseas and to expand DoD cyber cooperation with international partners.

The Department also continues to work alongside its interagency and international partners, in bilateral and multilateral engagements, to promote international norms for responsible state behavior in cyberspace. Doing so helps to set expectations for state behavior and makes it easier to recognize when malicious state actors engage in behavior outside those boundaries. The Department actively supports the Department of State in the United Nations Open-Ended Working Group as well as in the Group of Governmental Experts, both of which are tasked to look at how international law applies in cyberspace and what are appropriate standards of responsible state behavior.

The Department must also ensure that our allies and partners are aware of the national security risks that result from relying on vendors that lack good

security practices or that can be unduly influenced by state or non-state actors. We work closely with our allies and partners to illustrate the total costs of ownership of subsidized networks, such as those offered by Huawei, as well as the long-term impact on their security and economic competitiveness. The Administration has made it a priority to communicate the security threats presented by manufacturers of concern to our partners, particularly where it stands to impact our bilateral cooperation and information sharing.

**The Future: Budget Overview**

The FY 2021 President's Budget is designed to build on the progress we made last year towards implementing the 2018 DoD Cyber Strategy by enhancing our defensive and offensive capabilities. The Department's request of $9.8 billion for the Cyberspace Activities budget represents an increase in cyberspace funding of $0.2 billion compared to the FY 2020 budget request. These enhancements will reduce risk to DoD networks and to systems and information, and they will continue to grow our warfighting capabilities.

**Conclusion**

Thank you once again for the opportunity to appear before you today. With the 2018 National and DoD Cyber Strategies in place, we are confident that the Department has the right policy, guidance, and funding levels to support the defense of our Nation in cyberspace. The Department has made tremendous

strides towards achieving our national objectives in cyberspace since I last appeared before this Subcommittee a year ago. Cooperation across the Executive Branch and with our private sector and international partners has reached new heights, we have begun to use our expanded authorities to enable our mission to defend forward, and, through the efforts of the OPCA, we continuously aim to ensure that the elements necessary for the success of the overall strategy are properly aligned. Although challenges lie ahead, I look forward to working with you and our critical stakeholders inside and outside the U.S. Government to ensure that the U.S. military continues to compete, deter, and win in cyberspace.

**Kenneth P. Rapuano**
**Assistant Secretary of Defense for Homeland Defense and Global Security**

Mr. Kenneth P. Rapuano is the Assistant Secretary of Defense for Homeland Defense and Global Security. Previously Mr. Rapuano was a Senior Vice President at the ANSER Corporation, and the Director of the Studies and Analysis Group which provided multi-disciplinary studies and operational analysis for a broad array of government clients in the national security, homeland security areas. Up until November of 2016, Mr. Rapuano Directed the Homeland Security Studies and Analysis Institute (HSSAI), a Federally Funded Research and Development Corporation (FFRDC) operated by ANSER, a mission oriented not-for-profit organization.

Prior to joining ANSER Mr. Rapuano was the Director of Advanced Systems at the MITRE Corporation. He was responsible for guiding crosscutting strategic national and homeland security mission initiatives, with particular focus on counterterrorism, intelligence, aviation security, crisis management/decision support, national preparedness, and CWMD.

Previously, Mr. Rapuano served at the White House as Deputy Homeland Security Advisor to President George W. Bush from 2004-2006. He was responsible for managing the development and implementation of homeland security policies among departments and agencies, chaired the Homeland Security Council Deputies Committee, and co-chaired the White House Counterterrorism Security Group. He left the White House in 2006 to volunteer for deployment as a Marine Corps officer to Afghanistan with a Joint Special Operations Task Force, establishing and directing a targeting fusion center tracking high-value terrorists and insurgents. He also served in Iraq in 2003, commanding the Joint Interrogations and Debriefing Center of the Iraq Survey Group established to conduct the mission of surveying and exploiting possible weapons of mass destruction activities across Iraq.

In 2003, Mr. Rapuano was appointed Deputy Under Secretary for Counter Terrorism at the Department of Energy, responsible for nuclear counter terrorism, homeland security, emergency response, and all related special access programs for DOE and the National Nuclear Security Administration. Previous to that, he was the National Security Advisor to the Secretary of Energy. Mr. Rapuano has also served as Special Assistant to the Assistant Secretary of Defense, International Security Policy. He served 21 years on active duty and in the reserves as a Marine Corps infantry officer and intelligence officer.

Mr. Rapuano has also served as a Distinguished Research Fellow at the National Defense University's Center for the Study of WMD, as a member of the Defense Science Board Task Force on the Role of DoD in Homeland Defense, the Pacific Northwest National Lab's National Security Advisory Committee, the FBI's Weapons of Mass Destruction Directorate Advisory Group, the DHS Quadrennial Homeland Security Review Advisory Committee, and the DHS Science and Technology Advisory Committee.

Mr. Rapuano received a bachelor's degree in Political Science from Middlebury College, a master's degree in National Security Studies from Georgetown University, and has attended the Marine Corps Air-Ground Task Force Intelligence Officer Course at the Navy and Marine Corps Intelligence School.

STATEMENT OF

GENERAL PAUL M. NAKASONE

COMMANDER

UNITED STATES CYBERSPACE COMMAND

BEFORE THE

HOUSE COMMITTEE ON ARMED SERVICES

SUBCOMMITTEE ON

INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

4 MARCH 2020

Chairman Langevin, Ranking Member Stefanik, and distinguished members of the Committee, I am honored to appear before you today to discuss the accomplishments of United States Cyber Command (USCYBERCOM) over the last year and to discuss its future. It has been ten years since the Department of Defense created Cyber Command and began investing in its success. Today, I want to reflect on three areas where Cyber Command offers a return on those investments in line with the priorities of the National Defense Strategy. Cyber Command:

1. Imposes tailored, non-kinetic costs on adversaries, contributing to the lethality of the armed forces;
2. Expands military-to-military relationships, contributing to more effective partnerships for the armed forces; and
3. Innovates to address hard internal problems, reforming our business practices.

These returns on the nation's investment in Cyber Command are made possible by a professional force of soldiers, sailors, airmen, marines, civilians, and contractors. It is a force whose readiness continues to improve.

USCYBERCOM performs three main missions: it defends the military's networks, it supports the broader joint force with cyber operations, and it defends the nation from significant cyber attacks. It executes an FY20 budget of $596 million and has requested a budget of $638 million for FY21. Its full-time personnel total 1,778 military and civilians, plus contractors. In January 2020, we rostered 5,094 active duty service members and civilians in the Cyber Mission Force (CMF).

A decade ago, we trained and postured our cyber forces like any other military force: to prevail in future conflict. A central challenge today is that our adversaries compete below the threshold of armed conflict, without triggering the hostilities for which DoD has traditionally prepared. That short-of-war competition features cyber and information operations employed by nations in ways that bypass America's conventional military strengths.

The Chinese Communist Party (CCP) use of political repression and economic coercion – particularly through forced tech transfers and state-sponsored commercial espionage – harms U.S. interests and undermines the sovereignty of our allies and partners. Russia's efforts to undermine western institutions and to intimidate its neighbors have showcased its willingness to launch destructive cyber operations and pervasive influence campaigns. The latter remains the top concern when it comes to the 2020 elections, a topic to which I will shortly return. Iran has conducted disruptive cyber attacks against U.S. companies and partners, and employs similar tactics, along with information operations, to push its own narratives across the Middle East. North Korea uses cyber operations to steal currency that it would otherwise be denied under international sanctions. Violent extremist organizations also have used the Internet to command and control forces, to recruit, and to spread terrorist propaganda.

In 2018, "defend forward" became the cornerstone of DoD's cyber strategy to deal with the threats I've just described. It set an important tone for the joint force, stressing just how serious these threats have become to the military, and to encourage disrupting these threats before they harm the nation. This strategic direction drives Cyber Command's doctrine called persistent engagement: it enables partners with unique insights, and it stands ready to act by imposing costs when authorized.

*Cyber Command imposes tailored, non-kinetic costs on adversaries, contributing to the lethality of the armed forces.*

Cyber Command contributes to the broader joint force's ability to impose costs through hunt forward missions, offensive cyber operations, and information operations. First, I will describe how cost imposition fits in to our support to the whole-of-government effort to protect the 2020 elections. Second, I will describe how Cyber Command increases the lethality of other combatant commands. Third, I will explain how Cyber Command's defensive cyber operations improve the resilience of the military's networks, which forces adversaries to expend resources for diminishing returns.

**Defend the Nation and Election Security**

Today, we are 244 days from the 2020 Presidential election. Last year, we institutionalized our efforts from the Russia Small Group before the 2018 elections into an enduring Election Security Group for 2020 and beyond. The group reports directly to me and is led by representatives from Cyber Command and the National Security Agency. Its objectives are to generate insights that lead to improved defenses and being prepared, if ordered, to impose costs on those who seek to interfere. To be sure, we place a high priority on collecting and sharing information with our partners at DHS and FBI to enable their efforts as part of a whole-of-government approach to election security. But Cyber Command's authorities mean that it must also be prepared to act.

In 2018, these actions helped disrupt plans to undermine our elections. During multiple hunt forward missions, Cyber Command personnel were invited by other nations to look for adversary malware and other indicators of compromise on their networks. Our personnel not

only used that information to generate insights about the tradecraft of our adversaries, but also to enable the defenses of both our foreign and domestic partners. And by disclosing that information publicly to private-sector cybersecurity providers, they took proactive defensive action that degraded the effectiveness of adversary malware.

Cyber Command also executed offensive cyber and information operations. Each featured thorough planning and risk assessments of escalation and other equities. Each was coordinated across the interagency. And each was skillfully executed by our professional forces. Collectively, they imposed costs by disrupting those planning to undermine the integrity of the 2018 midterm elections.

Cyber Command's contributions to broader government efforts to protect elections are part of its mission to defend the nation in cyberspace. To defend the nation from this and other kinds of malicious cyber activity, persistent engagement with our adversaries allows Cyber Command to generate new insights that drive new methods of defense, and inform future options to impose cost. This approach drives the Election Security Group's approach to the 2020 elections, ensuring that exquisite intelligence drives tailored operations, which in turn generate more insight and opportunities to harden defenses and impose costs if necessary.

**Support to Combatant Commanders**

While persistent engagement drives Cyber Command's defense of the nation in cyberspace, the command simultaneously works with my 10 fellow Combatant Commanders to support and enable their efforts as part of the joint force. That support improves the defenses of their portions of DoD's networks and makes each command more lethal in its missions. Our

new Cyber Operations-Integrated Planning Elements (CO-IPEs) allow for greater integration into each command's operations.

As an example of how Cyber Command supports other joint force commanders, consider the support Cyber Command provides to U.S. Special Operations Command. The Marine Corps is the service that supports SOCOM, so MARFORCYBER provides the team of uniformed and civilian personnel that comprise the CO-IPE at SOCOM. The team's presence at MacDill Air Force Base and other SOCOM locations allows it to understand and facilitate SOCOM's dynamic requirements for cyber support to accomplish its missions. The CO-IPE also offers lessons learned and new options to SOCOM planners based on insights from fellow CO-IPEs at other commands.

To extend this example to the battlefield, MARFORCYBER's Joint Task Force-ARES has imposed costs on violent extremists online to support the overall counter-terrorist mission. ISIS is now mostly confined to publishing text-only products, instead of their previous, gruesome multi-media products. These products used to be disseminated in multiple languages through mass-market platforms. Now, ISIS struggles to publish in non-Arabic languages and is confined to less-traditional messaging applications. Of course, the collapse of the physical caliphate made it harder for ISIS to operate online. But Cyber Command's efforts through JTF-ARES remains important to contesting ISIS's attempts at establishing a virtual caliphate as well.

For years, Cyber Command has supported Central Command objectives in Iraq and Afghanistan, especially with information operations to protect U.S. and allied forces. As the entirety of the Department of Defense reorients around the 2+3 construct, so too have our efforts to provide cyber support.

**Defensive Cyber Operations and Resilience**

A third way Cyber Command imposes costs on adversaries is by improving the resilience of military networks. By taking preventive measures, we try to limit the incidence of network compromises. By being more rapid with our incident response, we aim to detect, quarantine, and expel intruders in as short a time as possible. By expediting network reconstitution, we can restore functionality to return the force to mission faster. By making the DODIN harder to compromise, and by reducing the operational impact of compromises, our networks are becoming more resilient. This imposes a cost on adversaries because they must expend greater resources, only to reap diminishing returns. My priority for defense in 2020 is to emphasize a command-centric model so that our network defenders are threat informed and our leaders are accountable for the security of the networks they operate.

*Cyber Command expands military-to-military relationships, contributing to more effective partnerships for the armed forces.*

So much of Cyber Command's success reflects and informs close partnerships it has built across the U.S. government and with industry and academia. Over the last year, I have placed a particular emphasis on expanding military-to-military partnerships. In part, this is because such partnerships are critical to the joint force as a whole. However, the return of great-power competition, and how that competition manifests in cyberspace, makes it all the more prudent to work with our allies on activities that promote collective security.

Just as the partnerships with the United Kingdom, Australia, Canada, and New Zealand anchor NSA's foreign engagement, so too do relationships with several of these countries form

the bedrock of Cyber Command's international partnerships. But Cyber Command has a more expansive partnership agenda, starting in the Pacific. Many nations there have grown increasingly concerned by the malicious cyber activity they have encountered. Last year, I had the honor of visiting my counterparts in Japan and South Korea. Each is making impressive strides towards growing the capability to better protect their networks from cyber intrusions and compromise. Our militaries have important shared equities, so improving common network defense, expanding combined training, and sharing lessons and vulnerability information is of mutual benefit.

It has been heartening to see the maturation of how our partners in Europe are organizing for cyber defense. Cyber attacks in Europe have been a concern for over a decade. In October, I met with 30 of my counterparts for consultations and presentations. We discussed education, mission planning, training, exercising, and operations. I was impressed to see the importance they placed on thinking through the long-term investments required to build professional forces, capable of making material contributions to combined cyber operations.

What is also clear is that in cyberspace, just because a partner is located in one theater of the world does not mean the value it brings to a partnership is limited to that theater. Our adversaries have aspirations for influence and control that transcend geographic boundaries. So too must the utility of our partnerships. A partner in the Pacific, for example, might be ideal to work with to counter a threat in the Middle East. Indeed, this logic informs an initiative Cyber Command undertook with Southern Command last year to improve the cyber capacity of several South American partner militaries. In August of 2019, our forces built a network in country to simulate and test defensive tactics. This kind of capacity building is also augmented by the National Guard's State Partnership Program. The partnership between the Maryland Guard and

Estonia, for example, allows for longer-term relationships to be formed, which builds greater familiarity with the partner's infrastructure. With that familiarity comes trust and experience, which leads to tailored exercises that inform more actionable lessons learned.

The global connectivity that the Internet powers therefore creates new opportunities for military-to-military partnerships, and Cyber Command will be at the forefront of making those partnerships count for the joint force.

*Cyber Command innovates to address hard internal problems, reforming our business practices.*

Cyber Command has a special responsibility and opportunity to embrace innovative solutions to reform the way we do business. I'll discuss three of these efforts: the work enabled b a facility called Dreamport, our new Command Acquisition Executive, and our approach to capability development under the Joint Cyber Warfighting Architecture (JCWA).

Dreamport originated from Cyber Command's $4 million investment in a partnership with the Maryland Innovation and Security Institute (MISI), a non-profit organization. MISI operates Dreamport, as part of a 44,000-square foot unclassified collaboration venue. Having an unclassified space may not seem like much, but it is crucial to working with companies and other non-government entities like academics and researchers who lack the requisite clearances to work on the NSA campus. Many of our cybersecurity challenges are not unique to DoD: we can learn much through outside engagement, and Dreamport has brought that engagement to fruition.

Over the past 18 months, Dreamport has allowed the Command to engage more than 1,000 private companies, educate over 1,000 military personnel on innovative technologies, and involve more than 350 students and interns from 65 colleges and high schools on STEM initiatives. It has been home to Cyber Command's effort to begin implementing the principles of

zero-trust networking on the military's networks. Dreamport also hosted the public-private collaboration that resulted in kits that help enable the Cyber National Mission Force to conduct Hunt Forward operations. The traditional ways of doing business would have been too cumbersome and too slow. Dreamport is key to the command's ability to engage in public-private partnerships at the unclassified level.

If Dreamport provides the venue and the mechanism, then our Command Acquisition Executive (CAE) is our senior leader for those efforts. Last year, Cyber Command hired its first CAE, a member of the Senior Executive Service, to lead our team of innovators and capability developers. She executes her responsibilities under Cyber Command's acquisition authority to rapidly develop and deliver joint cyber capabilities. During FY19, the Command executed 81 contracting actions valued at $74.9M, staying within the $75M ceiling. The CAE is also establishing a JCWA integration office and is working with OSD and services to synchronize critical cyber capability development.

To enable our personnel to achieve their missions, Cyber Command works with the Services to develop the JCWA. It will allow Cyber Command to employ its forces to conduct offensive and defensive operations against common objectives regardless of service and physical location. To do so, Cyber Command needs: sensors for situational awareness; a Unified Platform to manage, store, and analyze data; Joint Cyber Command and Control for mission planning and execution; tools for cyber operations; a Persistent Cyber Training Environment to train and rehearse missions; and a Joint Common Access Platform from which to perform operations.

For example, the Rapid Capability Development Network is one of the most promising platforms for tool development. It allows developers and operators to co-locate and produce,

test, and deploy capabilities. When paired with the Army's mission rehearsal environment, cyber mission teams can develop, test, and rehearse to ensure that the desired operational effects are available if and when a mission is authorized.

*A Professional Military Cyber Force*

None of what I have described thus far is possible without the professional forces under my command. With the Cyber Mission Force reaching Full Operational Capacity in 2018, Cyber Command headquarters, together with the service cyber components, are improving the CMF's readiness. Ensuring the force is ready, trained, and equipped to impose costs on our adversaries was my top priority last year. To that end, Cyber Command standardized readiness metrics across the services for Cyber Protection Teams, and is currently establishing standards for the Cyber Mission Teams and Cyber Support Teams. Additionally, the Command is working with the services to review the team structure to ensure that capability and capacity reflects the National Defense Strategy's prioritization of the 2+3 threat construct.

The return on investment the cyber force has brought over the last several years is a direct result of the accomplishments of the talented cyber workforce provided by the services. Talent management is key. We have learned that financial incentives retain people, but not necessarily the most talented people. Keeping the best of the best focused on the hardest but most rewarding aspects of our unique missions is one of our best retention tools. Over the coming year we will engage the services to continue building a manpower model to support retaining the most talented professionals.

One of the most impactful components of that manpower model is the reserve component. Like in other domains of warfare, forces in the reserve component can augment active duty forces for Title 10 missions. Members of the Air National Guard augment a full time National Mission Team and two Cyber Protection Teams. The Army National Guard mobilizes over 150 cyber personnel to defend Army infrastructure as Task Force Echo. For additional cyber capacity, the Army is building 21 Cyber Protection Teams across the Reserve and Guard. The Air Force Reserve and Navy Reserve provide additional augmentation to active duty Cyber Protection Teams and Combat Support Teams. Their value to the nation is increased by the leadership and experience of so many of these individuals in the private sector. Since over 80% of critical infrastructure is in the private sector, members of the guard and reserve are a valuable source to bridge the knowledge between the government and private sector. There is much experience to be shared between the C-suite and the command suite.

The Cyber Excepted Service hiring authorities have helped the Command recruit skilled civilians with competitive compensation packages and faster hiring decisions. USCYBERCOM can now recruit talent directly at job fairs, which we have hosted at Fort Meade, Baltimore, San Antonio, and Silver Spring, Maryland. The Cyber Excepted Service has also led to shorter hiring timelines, allowing the Command to compete for talent by citing its nearly unique status as an employer in which personnel work as cyber warriors and perform or support full-spectrum cyberspace operations on behalf of the nation.

Distinguished members of the committee, I look forward to discussing these and other topics with you. Thank you again for inviting me, and especially for your support. I am happy to answer 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."

## QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MARCH 4, 2020

## QUESTIONS SUBMITTED BY MR. SCOTT

Mr. SCOTT. When it is time for service members to leave Active Duty, either through retirement or voluntary separation, they often seek and take employment in industry because of a federally mandated 6-month cooling-off period before they can be hired as Federal civilian employees. Should this restriction be relaxed or waived entirely for these well trained and fully credentialed military cyber professionals?

General NAKASONE. Recruiting and retaining top talent is my core priority for building the force at U.S. Cyber Command. I am also committed to ensuring that hiring decisions are undertaken fairly and within the letter and spirit of existing laws and regulations. I support the DOD legislative proposal to amend the statute to allow the hiring of retired military information technology (IT) and cyberspace professionals to DOD IT and cyberspace positions without the 180-day cooling-off period.

Mr. SCOTT. What is the relationship between the U.S. Cyber Command and the United States Coast Guard? What impact does the Coast Guard's aging IT infrastructure have on their ability to secure their networks against the latest cyber threats?

General NAKASONE. The Coast Guard Cyber a service component of U.S. Cyber Command and also a critical bridge with the Department of Homeland Security. The Coast Guard's Cyber Protection Team offers capacity to support the Coast Guard's defensive missions and protect their IT infrastructure from cyber threats. CG Cyber has 28 members detailed to USCYBERCOM headquarters, who carry out responsibilities in support of global cyber operations, long-term planning, exercises, and training. The Commandant of the Coast Guard has launched an effort to prioritize addressing the Service's aging technology infrastructure, and remains committed to defending its portion of the DODIN in accordance with the direction set by USCYBERCOM. The Service is fully equipped and postured to protect its mission critical cyber terrain and effectively leverages its relationships with DOD and DHS to thwart adversaries and emerging threats.

Mr. SCOTT. Should some of the recruiting standards be relaxed to recruit future cyberwarriors?

General NAKASONE. The military services do an exceptional job of recruiting talent to man the uniformed portion of cyber mission force. I have no issues with service-specific recruiting standards. I, along with the Service Cyber Components, have the ability to recruit civilians directly through the Cyber Excepted Service, where military recruiting standards do not apply.

Mr. SCOTT. You mention in your testimony that violent extremist organizations also have used the internet to command and control forces, to recruit, and to spread terrorist propaganda. What about the VEO's use of the internet for fundraising?

General NAKASONE. Violent Extremist Organizations use a variety of methods to fundraise, including Internet-based techniques. Joint Task Force Ares is the component of U.S. Cyber Command that leads efforts to counter violent extremist activity online. They work with partners throughout the federal government to generate insight about the tactics of these extremists, and they support the development of options to counter them.

Mr. SCOTT. How does CYBERCOM leverage commercial threat information providers? How does CYBERCOM share information?

General NAKASONE. USCYBERCOM leverages commercial threat information providers in three important ways. First, companies offer finished reports about cyber actors and their tactics derived from data they collect and research they conduct. This kind of finished reporting supplements USCYBERCOM's analytic understanding of our adversaries. Second, companies provide access to structured datasets that help USCYBERCOM conduct deeper research. Finally, other companies offer a stream of structured event data that can improve situational awareness of real-time threats. While some contracts limit how USCYBERCOM can share data, USCYBERCOM elements can blend information from many providers into aggregate products that can be shared with other partners.

Mr. SCOTT. The Cyber Mission Force has long been comprised of approximately 6,100 personnel, is this the right size, given the demands of the nation?

General NAKASONE. The strategic environment has changed since the standup of the CMF in 2012. Over this coming year, USCYBERCOM, in partnership with the Joint Staff and Department of Defense, intends to gather data and assess how the CMF force aligns with and should be sized to meet the current missions it must execute.

○