Stenographic Transcript
Before the

Subcommittee on Cybersecurity

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

CYBER POSTURE OF THE SERVICES

Tuesday, March 13, 2018

Washington, D.C.

ALDERSON COURT REPORTING

1155 CONNECTICUT AVENUE, N.W.

SUITE 200

WASHINGTON, D.C. 20036

(202) 289-2260

www.aldersonreporting.com

HEARING TO RECEIVE TESTIMONY ON THE CYBER POSTURE OF THE SERVICES IN REVIEW OF THE DEFENSE AUTHORIZATION REQUEST FOR FISCAL YEAR 2019 AND THE FUTURE YEARS DEFENSE PROGRAM

Tuesday, March 13, 2018

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

The subcommittee met, pursuant to notice, at 2:31 p.m. in Room SR-222, Russell Senate Office Building, Hon. Mike Rounds, chairman of the subcommittee, presiding.

Members Present: Senators Rounds [presiding], Sasse, Nelson, McCaskill, Gillibrand, and Reed.

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

Senator Rounds: -- of each branch of our Armed Forces, from Vice Admiral Michael Gilday, Commander, Fleet Cyber Command; Lieutenant General Paul Nakasone, Commander, Army Cyber Command, and nominee to be the next Commander of the United States Cyber Command, and Director of the National Security Agency; Major General Loretta Reynolds, Commander, Marine Forces Cyber Command; and Major General Christopher Weggeman, Commander, Air Force Cyber.

At the conclusion of Ranking Member Nelson's remarks, we will ask our witnesses to make their opening statements. After that, we'll give each of our members 5 minutes to ask questions of our witnesses.

As we approach full operational capability later this year, maturation of the Cyber Mission Force continues at an impressive pace. According to Admiral Rogers' testimony a couple of weeks ago, we are on pace to reach that milestone earlier than planned. This, along with the many other advances we see as the Department takes what was once a niche capability and transforms it into a multifaceted warfighting discipline, is the result of your hard work. We thank you for your leadership.

Despite the successes, however, challenges remain as your focus now shifts from building a first-of-its-kind

force to a sustaining one. In particular, that sustainment will require a robust pipeline of talent ready to take the reins as soldiers and civilians move to other disciplines, are promoted, or separate from the military to take cyber jobs in the private sector.

Last year, we heard about the 127 Air Force cyber officers who, after completing their tour on the Cyber Mission Force, departed the Cyber Mission Force. We understand that was an isolated incident and that each of the services has enhanced its focus on how it manages it force. Just recently, the Marine Corps announced that it was creating a cyberspace occupational field to address some of these challenges. I think we all expect this to be a perpetual challenge, and we look forward to hearing how you are working together, sharing ideas, and pursuing creative approaches to make certain that we develop the bench strength that we require.

When it comes to providing the cyberweapons that the force will need to deter and defend its cyberspace, there, too, is significant room for improvement. As we heard from Admiral Rogers a couple of weeks ago, we are not where we need to be. Numerous niche capabilities exist today; however, across the enterprise, the capabilities for training and conducting operations are in the earlier stages of development and won't be delivered for some time. The

force will undoubtedly be hollow in the near term, and it is incumbent upon each of you to deliver those fundamental tools and capabilities as quickly as possible to make certain that the impressive gains you have made in training the force are not lost because of this lack of cyberweapons. We have been largely critical of the Department regarding this failure in the past, but we do see progress.

The fiscal year 2019 budget requests included $1.8 billion for the manning, training, and equipping of the Cyber Mission Force. The Army and the Air Force requested approximately $700 million each in FY19. The Navy request, however, was only 318 million and is less than half the request of its peers. Both the Army and the Air Force have committed to developing foundational capabilities, like the Army's persistent cyber training environment and the Air Force's unified platform. We look forward to hearing more from the Navy and the Marine Corps as to why, legitimately, their funding requirements are substantially less than the other services.

I think our hearing would be incomplete without some discussion of the services' offensive and defensive cyber capabilities. Of particular interest to me is the services' offensive capabilities in the context of the report of the Defense Science Board Task Force on Cyber Deterrence, which was published in February 2017, just over a year ago. As we

know, that report notes the importance of a strong cyber deterrent for the next 10 years, a period during which we will not have the defensive capability to defeat our peer adversaries' offensive capabilities. I would be interested in how the services are focusing to meet that challenge and policy issues -- policy issues -- that may be inhibiting their ability to do so.

Finally, I would like to know how the services assess their capabilities to provide support to civil authorities.

Let me close by expressing our gratitude to the witnesses. Yes, issues do remain, but the progress made in the past 8 years is a testament to the advocacy and leadership of each of you and your predecessors. Thank you again for your service and your willingness to appear today before our subcommittee.

Senator Nelson.

STATEMENT OF HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

Senator Nelson: Thank you, Mr. Chairman.

And I want to hit three issues for you all to contemplate and to respond to.

The first is just how disorganized the Department of Defense is when it comes to information warfare or information operations. Officially, doctrine recognizes that information operations include cyber, psychological, electronic, and public affairs. There's even an organization called Joint Information Warfare Center. And at the level of the military services represented here today, there is some integration of all of these elements. But, above that level, these elements are all dispersed. Cyber Command doesn't have the responsibility for information operations, which, these days, are conducted largely through cyberspace. And information operations and electronic warfare are the responsibility of still other parts of the Department. Now, why does this matter? Because Russia's information operations troops conduct both technical and cognitive operations in an integrated way. We conduct information operations in support of commanders at the tactical level. Putin and other adversaries are coming at us at the strategic level in so-called peacetime. I'm afraid that we are ceding the playing field. And I look

forward to you all giving us your answers to this.

The second issue is the slow pace of progress in equipping the cyber units that we have built. We've manned and trained our cyber units, but we still lack basic joint capabilities for command and control, the clandestine network infrastructure needed to maneuver our forces in cyberspace, and the tools and weapons that they need.

And the third issue is, we have to squarely face the reluctance to use military cyber units to respond to attacks against us, to confront Russian hackers and trolls, to harass North Korean operators who attack Sony, and to disrupt ISIS Internet operations outside areas of declared hostilities. And we're not conducting our own information operations to defend against and to deter acts -- attacks and acts on us and our allies.

And this is not just about Russia. It's about differing views among all the parts of our government about what constitutes traditional military activities. We have to change this. Our forces can't just watch our adversaries in cyberspace. And I applaud General Weggeman for stating, in his prepared comments, and I quote, "We must challenge outmoded concepts of sovereignty, attribution, and intelligence gain/loss calculations which overly constrain our ability to achieve cyberspace superiority," end of quote.

We're all concerned about these threats, but that concern has not yet been matched by action. I want to hear what each of you think. And I realize, as stated to us by the four-star Commander of Cyber Command, he hasn't been given the direction. So, I understand the constraints that you have. But, we've got to get this out on the table. And I hope we can start today.

Thank you, Mr. Chairman.

Senator Rounds: Thank you, Senator Nelson. I think you do a good lead-in to a lot of not just the capabilities that we've got, but to the policy issues we have to address, as well.

I'm not sure how you would like to proceed, or in what order you would like to proceed. If there is a preference, I would allow our witnesses to make that determination.

Lieutenant General Nakasone, have you -- would you care to begin, sir?

STATEMENT OF LIEUTENANT GENERAL PAUL M. NAKASONE, USA, COMMANDING GENERAL, UNITED STATES ARMY CYBER COMMAND

General Nakasone: Thank you, Senator.

Senator Rounds -- Chairman Rounds, Ranking Member Nelson, and members of the subcommittee, it's honor -- it's an honor to be here, alongside my joint teammates, representing U.S. Army Cyber Command.

My testimony today focuses on the progress Army Cyber Command has made since May 2017, when I last sat before this subcommittee.

Today, the Army's 41 Active Cyber Mission Force Teams are fully operational, on mission, equipped, and delivering capabilities to joint and Army commanders in contingency operations across the globe. With the initial build of the Army Cyber Mission Force complete, our cyber is now focused on sustaining and measure readiness and building the Army's 21 Reserve-component teams. All 21 Reserve-component teams, which are now part of the Cyber Mission Force, will reach initial operational capability by 30 September 2022, and full operational capability by 30 September 2024.

We continue to make our networks more secure and more dependable through convergence, modernization, and standardization. A key priority is updating Army computers to a more secure operating system, a system known as Windows 10. Over the past 12 months, the Army has already upgraded

over 95 percent of its approximate 1 million computers.

Regarding training, the Army Cyber Center of Excellence is now teaching all cohorts from all components, and preparing to integrate the electronic warfare force into the cyber career field. The Army also continues to guide program management for the joint persistent cyber training environment. We are leveraging existing infrastructure and resources to integrate the best government off-the-shelf and commercial off-the-shelf solutions. Construction on the Army Cyber Command Headquarters Complex at Fort Gordon continues and is taking shape, transforming the Fort Gordon region into a cyberspace hub for the Army and the Nation.

Thanks to congressional support, Army talent management initiatives are also paying off. We will soon have the Army's first direct commissioned cyber officers, and our civilian cyber operators will have a new career management field. We are also incentivizing soldiers through expanded use of the assignment incentive pay and special duty assignment pay.

Partnerships remain critical to our efforts. We are leveraging the private sector, the academic community, and the key allies to rapidly develop and deliver new capabilities to the joint force and our Army.

In the future, the Army will require sustained investment in science and technology to capitalize on the

advancements in artificial intelligence and other innovative capabilities. We also need to pursue force structure and capabilities at the Army corps level and below to ensure we have the tactical capabilities our pilot initiatives have shown.

Today, the Army is driving hard to lay the groundwork for the future force. With Congress's support, we will continue to build upon our momentum to deliver a formidable cyber force to our warfighting commanders.

Mr. Chairman, I would request my written testimony be entered into the official record. And I'm happy to answer the committee's questions.

[The prepared statement of General Nakasone follows:]

Senator Rounds: Thank you. Thank you, Lieutenant General Nakasone.

And all of your complete messages or reports will be entered into the record, without objection.

Vice Admiral Gilday.

STATEMENT OF VICE ADMIRAL MICHAEL M. GILDAY, USN, COMMANDER, UNITED STATES FLEET CYBER COMMAND, AND COMMANDER, UNITED STATES TENTH FLEET

Admiral Gilday: Chairman Rounds, Ranking Member Nelson, Senator Sasse, good afternoon. On behalf of the sailors and the civilians of Fleet Cyber Command, it's an honor to be here with my joint teammates, and I thank you for the opportunity to appear. I also want to thank you for your leadership and for your support in helping to keep our Nation secure in this complex domain of cyberspace.

Since appearing before this committee last year, and like my fellow cyber component commanders, I have continued to observe an upward trend in the capacity, the capabilities, the sophistication, and the persistence of cyberthreats against our networks. Cyberspace intersects every one of our Navy's missions, and it requires an adaptive approach to counter the threat.

Navy's approach for offensive and defensive cyber can really be summarized in three broad areas: first, modernizing our existing networks; second, by investing in new technologies and partnerships; and lastly, by carefully managing our talent.

First, we are modernizing and defending our networks by implementing our cyber resilience strategy, focused on hardening our network infrastructure and reducing its attack

surface. We're in the fifth year of this ongoing effort. Further, we have extended our defensive posture to include deploying defensive cyber teams with our carrier strike groups and our amphibious readiness groups.

Second, we are investing in new technologies and partnerships for the offense and the defense through a series of initiatives, including transitioning to cloud-based technologies. At the same time, we are investing in improvements to defend and to gain better situational awareness deep inside our networks. We are leveraging the data sciences through the Navy's new Digital Warfare Office, and collaborating with industry and academia to apply new technologies, like machine learning and artificial intelligence. We continue to mature partnerships with a host of allies and partners. And we have established two new commands, one for doctrine development and the other for training, both improving the integration of cyberspace and electronic warfare into fleet operations.

Third, we're committed to growing and sustaining our talent base. Now that all 40 Navy cyber teams have reached full operational capability, we are focused, as Admiral -- as General Nakasone said, on sustaining a mission-ready force. We are meeting, and in some cases exceeding, accession and retention goals for both officers and enlisted, as well as expanding our direct-commission cyber

warrant officer and cyber warfare engineer programs to capitalize on our technical talent. We're improving the ways we integrate cyber talent from the Reserve force, and we are implementing the DOD's new Cyber Excepted Service Program for our civilian teammates. We are improving virtual training capabilities for all of our cyber teams, and we are building a new cyber center at the United States Naval Academy and offering graduate degrees for both officers and enlisted at the Naval Postgraduate School.

Lastly, I still believe we have much room to grow. In particular, we need to continue to seek improvements in how we recruit, how we train, how we retain, how we reward, how we fight, all the while ensuring that our forces are equipped to compete and defeat the adversary.

Mr. Chairman, Senators, thank you for the opportunity to be here this afternoon. I take the points from your opening remarks, and I look forward to answering your questions.

[The prepared statement of Admiral Gilday follows:]

Senator Rounds: Thank you, Vice Admiral Gilday.

Major General Reynolds.

STATEMENT OF MAJOR GENERAL LORETTA E. REYNOLDS, USMC, COMMANDER, MARINE FORCES CYBERSPACE COMMAND

General Reynolds: Good afternoon, Chairman Rounds, Ranking Member Nelson, Senator Sasse, and other members of the committee. On behalf of the marines, the civilians marines, and the families of the United States Marine Corps Forces Cyberspace Command, I want to thank you for your continued support, and I appreciate this opportunity to update you on the tremendous progress that we've made since I was last before you in May.

I'd like to highlight what our marines are doing in the cyberspace domain, and how we've shifted our focus from building the command to operationalizing, sustaining, and expanding capabilities in this new domain.

Chairman, at MARFORCYBER, I have organized operations along three lines of effort, and I will briefly highlight those for you today. I use this framework to organize my activities and to measure our progress.

So, my first priority is to secure, operate, and defend the Marine Corps Enterprise Network, the Marine Corps portion of the DOD Information Network. We have continued to expand our definition this year of the MCEN by including all elements of the Marine Corps IP space, which includes our many disparate networks that are owned and managed by different commands across the Marine Corps. To be more

defensible, we've collapsed domains this year, we've expanded our enterprise view of the network through a common service desk, an endpoint, discovery, and we are now -- as General Nakasone mentioned, we are also nearing completion of upgrade to WIN 10 across the Marine Corps. We've also experimented with additional acquisition methods and models like DIUx that are more responsive to the changing threat. And we're looking forward to employing Cyber Command acquisition authority, when it makes sense.

Moving forward and in response to the National Defense Strategy, we know we must be prepared to fight tonight, and we will build the objective network capable of fighting and winning against a peer adversary in a contested information environment. So, recognizing that our ability to command and control is our center of gravity, we are participating in efforts with the United States Marine Corps Service Headquarters to design and build a more defensible network architecture.

My second priority is fulfilling our responsibility to provide warfighting capabilities through the development of ready, capable cyberforces to United States Cyber Command. And I am happy to report that, as of January of this year, ahead of schedule, all of our 13 teams have reached full operational capability and are employed against priority missions. Many of our marines have participated in planning

or executing offensive and defensive missions against today's adversaries, and are informing tactics and procedures on a daily basis. We are increasing our proficiency every day.

And now, to increase readiness and retention, and to increase skills progression, sir, as you mentioned, the Marine Corps, just last week, announced the creation of our cyberspace occupational field. The creation of the MOS will allow us to deliberately provide targeted incentives for recruiting and retention. And, for our civilian marines, we are leaning into hire and transition our workforce to the Cyber Excepted Service. As part of our integrated planning element build in support of Special Operations Command, we have hired civilians across the SOCOM enterprise who are providing cyber intelligence and planning support for joint cyber fires.

My third priority is to provide support to the Marine Corps as it works to operationalize the information environment. As you are aware, the Commandant has modified marine formations to build greater capability in the information environment under the Marine Corps operating concept, and we are building additional DCO forces inside the MAGTF, experimenting with tactical cyber, and sharing lessons on the integration of cyber with other fires and other information capabilities. As we continue to increase

our capability and our capacity, we look forward to occupying our new operational headquarters on NSA's campus next month.

I want to again take the opportunity to thank Congress for the military construction funding that enabled the development of our new building. This building is much more than just administrative spaces. It will serve as a platform for training, command and control, planning, and execution.

I am incredibly proud of the strides that we have made in operationalizing cyberspace in support of the MAGTF and the joint warfighter since I was last before you in May.

Thank you, Mr. Chairman and members of the committee, for inviting me to testify before you today, and for the support that you and this committee have provided our marines and their families. And I look forward to continuing the dialogue and to answer your questions today.

Thank you.

[The prepared statement of General Reynolds follows:]

Senator Rounds: Thank you, Major General Reynolds.

Major General Weggeman, you are last because you are the youngest of the branches.

[Laughter.]

Senator Rounds: You may begin.

STATEMENT OF MAJOR GENERAL CHRISTOPHER P. WEGGEMAN, USAF, COMMANDER, TWENTY-FOURTH AIR FORCE, AND COMMANDER, AIR FORCES CYBER

General Weggeman: I think that's an honor.

Thank you, Chairman Rounds, Ranking Member Nelson, distinguished members of the subcommittee. Thank you for the opportunity to appear before you today along with my esteemed cyber colleagues. I look forward to discussing the Air Force's significant progress in advancing full-spectrum cyberspace operations and our contributions to joint operations.

I have the distinct honor to lead more than 15,000 total-force airmen and civilians operating globally as a maneuver-and-effects force in a contested domain delivering cyber superiority for our service and in support of our joint partners.

In this domain, threats are growing rapidly and evolving. Our adversaries are acting with precision and boldness, utilizing cyberspace to continuously challenge the United States below the threshold of armed conflict, imposing great costs on our economy, national unity, and military advantage. In this ever shifting and competitive terrain, we must remain vigilant with cyber hygiene, cybersecurity, and threat-specific defensive operations in order to compete, deter, and win.

The Air Force has invested in the creation, fielding, and sustainment of an ever increasing portfolio of cyber defensive and offensive capabilities. Specifically, seven cyber weapon systems designed to provide a tiered global defense of the Air Force information network; second, defensive cyber maneuver forces to actively defend key cyber terrain; and, last, offensive capabilities to provide all-domain integrated operational effects to combatant commanders.

The Air Force's Cyber Mission Force Teams are on track to achieve full operational capability by the end of FY2018. As of today, 35 of 39 Cyber Mission Force Teams have declared full operational capability. By comparison, highlighting our extensive progress, at this time, at this same hearing 10 months ago, we only had nine teams at FOC. Our four remaining teams are expected to declare FOC by June of 2018, concluding our build phase 3 months ahead of deadline.

Air Force Cyber trains and fights as a total-force team, harnessing the unique attributes and talents of all components -- regular Air Force, Air National Guard, and Air Force Reserve. Across 24th Air Force, we employ more than 11,000 full-time and part-time Reserve and Guard personnel providing support for training, intelligence, full-spectrum operations, command and control, and capability development.

For our Cyber Mission Force Teams, the Air Force has employed a built-in total-force strategy with 15 Air National Guard squadrons and a classic Reserve associates squadron providing additional trained and ready surge capacity in times of crisis.

Cyberspace operations are powered through partnerships, and 24th Air Force is wholly committed to strengthening our relationships with other Air Force partners, our sister services, interagency counterparts, combatant commanders, coalition allies, as well as civilian industry partners. Congressional support continues to be essential to our significant operational progress, and will only increase in importance as we move forward.

I will keep my opening remarks brief, as I have provided a comprehensive update for the committee in my written statement outlining in detail our significant operational improvements, specific initiatives, successes, and challenges, of course.

I am honored and humbled to command this magnanimous organization, and I am inspired every day by the innovative spirit, the patriotism, the sacrifice, and audacity of our Air Force cyber warriors. They are, by far, our Nation's most powerful cyber weapon system.

I look forward to your questions and the ensuing dialogue.

Thank you.

[The prepared statement of General Weggeman follows:]

Senator Rounds: Thank you, Major General Weggeman.

Senator Sasse has been a regular attendee at these, and yet he always seems to have to leave before he can ask any questions. And so, I'm going to defer my questions.

Senator Sasse, you may begin.

Senator Sasse: Being 101st in seniority has some downsides, it turns out.

[Laughter.]

Senator Sasse: Thank you, Chairman.

Thank you all for your service. Thanks for being here.

I'd like to talk about the Presidential Policy Directive 20. Does it work? And, if not, what's the conversation like between you all and DOD and the NSC about that? Could you talk us through, a little bit, about how long it takes in the process, from beginning to end? All of you, but, General Nakasone, if you want to start.

General Nakasone: So, PPD-20, or Presidential Policy Director 20, the methodology upon which we get approval for offensive cyberspace operations, is a work in progress, in terms of the way that we've approached getting approvals. I would say we have had a tremendous amount of success with ongoing operations with regards to JTF Ares and our fight against ISIS. That has been, certainly, something that has allowed us to make a case for the things that we need to have done. Is the process perfect? No, it's not. But,

this is a constant dialogue that goes on between ourselves, certainly Cyber Command, and the Department of Defense, and then the National Security Council, Senator.

Senator Sasse: Admiral.

Admiral Gilday: Sir, thanks for the opportunity to comment on this subject.

So, as General Nakasone mentioned, really we have not -- PPD-20 hasn't kept us from delivering effects when we have been required to deliver them. It is intended, or was intended, to be a very deliberate process in determining when and how we would deliver cyber effects against -- whether it's a sovereign nation or whether it's a rogue actor. And so, I think that -- as an overarching policy, I think that it's a good framework. There are built-in mechanisms within that framework to accelerate authorities if we need them. If the Nation needs to get authorities quicker, it exists.

But, as General Nakasone said, we have learned a lot in the last 2 and a half years. The world has changed a lot in the last 2 and a half years, in terms of how people act in this space. And so, I do think that we're learning from that, and I do think it's informing policymakers. And I think people are marching together to make improvements.

Senator Sasse: So, you can cite specific examples of times when the process has worked, but I assume, if we were

in a classified space, there would also be specific operations that you'd tell us about that you were never able to carry out because of how slow it is. I've heard other cyber warriors refer to PPSD-20 as molasses. Is it the case? And what can we talk about, in a nonclassified setting, about specific operations -- I guess not talking about specific operations, but what general takeaways do we have about times when it's been too slow to enable you to act in cases when you had targets that you would have liked to have pursued?

General Weggeman: Well, I can't speak to any of the operational specifics, but I'll give you a perspective, to your original question. And again, you know, policy is not my realm, as the senior military operational commander, but I'll give you some observations of PPD-20.

Now, when I first came into the domain in 2012, that's when we were writing PPD-20. So, think about the maturation and the pace of change since then. So, 6 years later, we still have the same PPD-20. It started out as kind of an authorities-driven policy directive. And I think what we're going to now is, we're learning now that we have capability, capacity to actually do more, we need more of a mission- and risk-informed policy that allows us a broader spectrum of authorities and risks that would allow us the pace, the timing and tempo of operations, I think, to match our

adversaries in cyberspace. So, I think that's where we're going now, that we're showing that we have capability, capacity, we're proving ourselves that we can be responsible and credible actors in this space. I think we should be looking at, How do we broader -- how do we create a broader spectrum of threat- and risk-based authorities and delegation so that we can respond with greater tempo.

Senator Sasse: I want to follow up on the standardized delegation question, but generally I think you were trying to get --

General Reynolds: Senator, I would -- I mean, I think what you've heard from the other Commanders is exactly that, in that everything that we are learning -- I think, every day, we are learning more and more about the delivery of effects in this domain. And, to General Weggeman's point, it's really a matter of, Where's the risk, and who should accept that risk and -- from a decisionmaking perspective? And so, I certainly think there's some room to have more discussion on this, on this PPD, sir.

Senator Sasse: If you were, sort of, briefing the Armed Services Committee on what standardized delegations might look like for all of our allies, could you give examples of cases where our allies might have some delegated authorities that have been routinized that you'd like us to look at?

General Nakasone: Certainly, Senator. And I'd -- I would welcome -- probably do that in a different session.

Senator Sasse: I think there are a number of us who'd like to follow up on that and be tutored by you. Again, with all respect to your operational responsibilities, not your policymaking responsibilities, but those of us who are in a policymaking role know well that we need the tutorials of people who are actually living this, day in and day out. So, I'm over time, here, but we'll follow up on that, and invite you back in a classified space.

Thanks.

Senator Rounds: Senator Nelson.

Senator Nelson: Mr. Chairman, we're here in the family, so you go ahead.

Senator Rounds: All right, thank you. And I appreciate it.

I'm going to follow up kind of along the same lines that Senator Sasse has begun. And I think it's a good line to begin with.

I'd kind of like to know what limitations and current policy most immediately challenge your ability to operate effectively in cyberspace, if I could. And I'll just open this up. We're all in the family here. And I recognize that we're in an open session, but we're talking about policy and the difference -- and let me perhaps preface this

a little bit.

We've got thousands of years of knowing how armies have learned how to interact with one another on a battlefield. There are norms that have been established. The same with the law of the sea. There are norms that have been established, in terms of how we treat one another, military to military, military to civilian, and so forth. Even in the air, we have norms about how one aircraft treats another aircraft when there are incidences involved. Space is perhaps a little bit newer. And, most certainly, the norms there have not been completely established.

When it comes to cyber, the norms are still being established. And our expectation, in many cases, is based upon what norms in other domains of war have already been established. It would seem that our adversaries have not taken the same approach and are not bound by the same respect for norms as perhaps we are.

So, let me bring this back. Again, what are the limitations, in terms of how we look at and how we view the norms, when it comes to our offensive capabilities? And what are the limitations that we respect that perhaps you would see in -- Senator Sasse has indicated our allies perhaps have other alternatives or other policies established. We have peer competitors that most certainly do some things that we would not consider to be appropriate

at this point, or we are restricted from doing. Do you have any examples of that or things that you have seen that have been frustrating to you with regard to their offensive movements that we simply do not do?

General Nakasone: So, Senator, normally we're a very talkative bunch. I would offer that we can provide the perspective of our operational lessons learned. And let me take it from that aspect, because I think that's an important piece.

So, when we look at the domain, there are really three things that I think all of us are very interested to have a discussion on. First of all is the discussion of risk. Who accepts the risk? What is the risk? How you describe the risk. What are the mitigations for that risk? They're elements that I think that we talk a lot about when we're -- when we are in discussions and planning for cyberspace operations.

Second thing is, What's the operational gain/loss? If we do this mission, or we don't do this mission, what is the opportunity cost for those actions?

And the third element, I would say, is, What's the intel gain/loss? That is obviously a question that is offered by many of us, and also those in the interagency. And I think that that is perhaps the area that all of us, based upon our operational experiences, have spent some time

with.

General Weggeman: Yes, Senator. I guess I -- I think I need to offer a thought, based upon Senator Nelson quoting my written statement, because I think this gets right to it.

So, you know, to me, the cornerstone document is our new National Defense Strategy, right? So, compete, deter, and win. So, if I was looking at, you know, a broad set of policies, you know, I don't want to act like the irresponsible actors. I think our -- we're a nation of laws. I think we, as military operational commanders, operate under the Law of Armed Conflict, rules of engagement, and special instructions so that we're credible and responsible in the disposition of our duties. But, I do think, if we want to compete, deter, and win in cyberspace, that we have to get, to General Nakasone's point, more oriented on mission outcomes and risk models and threat-driven operations that allow us to become the challenger instead of the challenged in this domain.

And so, all the things you mentioned, all the things I talk about, I do think we have to look at new approaches within the confines of our government and what we seek to do from a national perspective on things like sovereignty. To your point, right? There is no international airspace or water in cyberspace. Every piece of the domain is some manmade space that someone says is his or hers. And so, we

have to rethink that. I think we have to look at -- becoming the challenger is going to require us to be more of a 21st-century information operation, information warfare, cogent organization or group of interagency partners that wants to then, you know, do the things that are happening to us -- to impose costs, to deny benefit, to demonstrate stake, and to convey the legitimacy of those actions to our citizenry, as well.

Senator Rounds: Thank you.

Senator Nelson.

Senator Nelson: General Nakasone, you're going to be the Commander of U.S. Cyber Command, and it is now being upgraded to a combatant command. Have you thought about the possible unique role that you're going to be, that you may be one of the U.S. military establishment commanders that is actually in actual combat?

General Nakasone: Senator, if confirmed, certainly I will be thinking every single day about that, and I have been a bit over the past couple of weeks, as I've testified. I would offer, as I think to this future, it's informed by much of what I've learned over the past couple of years in command of Joint Task Force Ares. If I might --

Senator Nelson: Okay. Let me stop you there. Let me ask about that. Because, as the commander of Task Force Ares responsible for the operations to disrupt ISIS, and

specifically to disrupt ISIS on the Internet for their propaganda, recruiting, and command and control, the Task Force's performance in its first year was rated as poor. But, you have testified, "Performance has gotten a lot better." So, have you conducted operations in Task Force Ares designed to manipulate the thinking of ISIS adherence?

General Nakasone: Senator, yes, we have. We have conducted information operations. And I would offer that that's perhaps the piece of Ares that I've learned the most about, being able to provide a message, to amplify a message to impact our adversaries.

Senator Nelson: So, not just disrupting their networks, but also conductive -- cognitive information operations.

General Nakasone: Yes, Senator. And, in fairness, as you pointed in your opening comment, probably more at the tactical and perhaps operational level. But, I think that that's where it begins, understanding how you provide that message, the infrastructure that you need, the capabilities that are going to underpin your messaging.

Senator Nelson: So, are you using the Army's first Information Operations Brigade?

General Nakasone: Senator, yes, we are. Certainly that's one of the elements. And other elements for our joint force, to include our Marines, our Navy and our Air

Force, as well, Senator.

Senator Nelson: So, now you're moving to the strategic level overall, not just the Army's perspective. Are there lessons from this task forward -- the task force that can be elevated to the strategic level and applied to the information warfare threat from Russia?

General Nakasone: Senator, I think there probably are, in terms of the lessons that we've learned in Ares. And, while I'm a bit hesitant to apply a broad brush, let me offer three that do come to mind.

First of all, you have to start early. You indicated the first year was a difficult one for us. It was a difficult one for us, because we were trying to build an infrastructure, build capabilities, build talent.

The second thing I would offer is, there's nothing more powerful than having your own infrastructure, your own capabilities. One of the things that the Army has provided us is an infrastructure that we use.

And third thing is, it comes down to talent. Eighteen months ago, in a room of, you know, cyberspace operators across our entire force, if I would have asked the question, "Raise your hand if you've conducted an offensive cyberspace operation," out of 100 soldiers, sailors, airmen, and marines, maybe two or three would have done it. Today, nearly the entire room has got their hand up, Senator.

Senator Nelson: So, as you go on to be the four-star commander of a combatant command, Russia has at least some military units that combine technical cyberoperations and information capabilities. The DNI has testified that their operations are having strategic effects on us. That's from Dan Coats, the DNI. Do your information operations units have cyber skills?

General Nakasone: Our information operations units do have cyber skills, Senator.

Senator Nelson: So, if all these functions are integrated at the service level, why do we separate them at the unified command level and in the Office of Secretary of Defense?

General Nakasone: Well, Senator, I take your point. And I think that's where Section 1637 of NDAA FY18 is looking at, is, How do you bring that together? How do you have one look? And I believe that OSD is working that piece of it right now, Senator.

Senator Nelson: Okay. And, as you work that, then you've got to have an answer to the question, Who is responsible for strategic information operations, the kind of operation that Russia has conducted against us in our elections? Anything you can comment on that in this setting at this time, even though you don't have the fourth star?

General Nakasone: So, Senator, I will wait until the

OSD has completed that study there. I think that that's important as we take look and move forward over.

Senator Nelson: Okay.

I'll just close out, Mr. Chairman, by saying that it was so telling when Admiral Rogers, our four-star commander, of which General Nakasone will relieve when Admiral Rogers retires -- it was so telling that he said he's ready to do the attacks, but he has not been given the authorities. And I fear for American democratic institutions if we don't attack.

Thank you, Mr. Chairman.

Senator Rounds: Senator McCaskill.

Senator McCaskill: Thank you.

Well, I would just like to speak briefly to you about a couple of issues. One is recruitment and retention of the personnel that we need in terms of the cyber fight. You know, there are many things about the Defense Officer Personnel Management Act that I think enhances the strength of our military, but there's also some things about it that don't seem to make much sense in certain contexts. And I really would love to get your all's input to how the up-or-out issue relates to the expertise we need in cyber. You know, I know that pilots in the Army can typically be warrant officers who can progress in rank but still continue to fly. Have we made the adjustments for cyber warriors to

be able to adjust in rank and still be able to work in the cyber sector? Or are we defaulting to the norm, which is moving them out of that MSO into something different so that they can get experience throughout the various parts of our excellent military?

So, I'd like each of you to address briefly the recruitment-and-retention issues and what issues that DOPMA may be causing for our retention of the very best in this really challenging field? We have enough trouble competing with the private sector without adding in some of the challenges that are inherent in the current way that we develop leadership in our military.

Admiral?

Admiral Gilday: Senator, good afternoon. Thanks for your question.

So, if I could say real briefly, in terms of constraints, I think we have direct commission programs now, where we're trying to attract the best and the brightest from society to join us. And so, their entry level is at an ensign or a second lieutenant. And so, that pay is about $37,000 a year base pay. So, we are not competitive with the private sector, in terms of competing for that kind of talent. And we want to go after it. Similarly --

Senator McCaskill: I get -- I mean, you know, we can't -- I mean, that's what we pay somebody to answer the phones

in -- around here. And we're asking them to have incredible expertise. That seems to me totally unrealistic.

Admiral Gilday: Yes, ma'am. And there have been other hearings on the Hill recently where this has been addressed by the personnel chiefs, in terms of requesting additional relief so that we can give people credit for their years of service in the outside sector and pay them what they deserve, in terms of being competitive with the private sector.

In terms of up-or-out, we have not made any modifications yet, although we know we're going to have to take a look at that and do so in the future. Because, to your point, we're just going to hemorrhage talent at that -- at those upper ranks, when we really don't need to. We could retain those people longer.

If I could talk about the civilian force for a moment, that's where we do have some challenges, in terms of some fairly rigid guidelines that we have to follow, in terms of the amount of incentives that we can offer people coming in. Maybe a 10-percent hiring raise, maybe a 10-percent relocation bonus; perhaps, in some cases, accelerated promotion -- but, not broadly enough to make us a very attractive employer for those in the private sector.

I think that the Cyber Excepted Service is a step in the right direction, in terms of providing us more latitude.

But, I still think the -- I still think that we will likely need more authorities to remain competitive, or to be competitive, with the private sector.

Senator McCaskill: Is there any other input that anyone would like to give on this subject?

General Reynolds: Senator, I would just say that I agree with everything that Admiral Gilday said. I think cyber is going to be the game-changer for us. We, in the Marine Corps, just established the new MOS so that we could target incentives. Already, I think, we're going to maximize the bonus structure that we have inside the Marine Corps to kind of get after and retain some of this special talent. The Commandant makes the point all the time, you know, "We may end up with a platoon of warrant officers, and that's got to be okay with us." So, I know, at the highest level of our service, he's willing to challenge status quo. And the key for us is to figure out, What exactly is that incentive? In some cases, ma'am, it's not pay. Sometimes it's education, sometimes it's certificates, sometimes it's -- you know, so, for us, it's being able to target those incentives and have the freedom of action to do that to retain the best talent, ma'am.

Senator McCaskill: Anybody else?

General Nakasone: I would add to General Reynolds' point. For the Army, what we have taken a look at is our

career fields. So, Senator, as you discussed the challenge with DOPMA right now, you know, up or out, what we have looked at is, Is there a career field out there for a tool developer that all he's going to do for 20 years is develop these exquisite tools? We think there is. One of the things that I have seen, across all the services, the senior leadership to, you know, try new flexibility on these things. Are we going to send enlisted soldiers to get a graduate degree? Are we going to send them to training with industry? Are we going to do different type of activities that will be attractive to them? Not all of them will work. Some of them will. But, unless we try some of these things, I think that, you know, we're going to have a challenge in the future.

Senator McCaskill: Well, if you have the flexibility with MOS descriptions and MOS incentives, then that's one thing, but I would really appreciate -- if there are things that we could add to the NDAA this year to give you more tools to recruit and retain -- there is no question that, if there is one area that I pretty much believe, on a bipartisan basis, everyone realizes that we have got to up our game, it is in cyber warfare, because clearly, right now, I would not say that we're winning. And I don't like it when we're not winning. And so, some of that is complicated by policy decisions, but some of it is us

getting the very best and the very brightest.

And so, if there are specific things we could do to give you additional flexibility or tools, I'd really appreciate it if you would share them with us before we begin our consideration of the NDAA this year.

Senator Rounds: I recognize that you are over on time, but I know that General Weggeman had tried to make a comment, as well, and I would allow General Weggeman to respond, as well, if he'd like to at this time.

General Weggeman: Yeah, I think my compatriots provided most of the responses. For me, I personally believe the services recruit, first, based upon values, and then, second, based upon talent or skillset. And so, I think the cornerstone we have as cyberspace operations professionals is our mission. As you all know, we're the only organization that has the mission to do what we do, when directed and authorized, legally. And so, I look at that as the biggest retention tool we have. Is like -- it's like young Captain Weggeman on the F-16 line. When I flew four times a week, I was as happy as they get. Give me any mission, send me anywhere. I'm up for it. It's the same for our cyber operations professionals. You know, reps and sets. So, we have to make sure we're giving them the tools, the infrastructures, and the environments so that they can sharpen and hone their tradecraft, so they get those

sorties. And that helps with retention, for sure.

But, you know, the second thing that would help us all is, we're all working together. I think we're working with industry on cutting-edge assessment tools to assess a cyber aptitude of an individual when they come in front of us. What -- you know, the interesting I -- thing I learned from the people -- again, I'm not a technologist, ma'am, I'm a fighter pilot by training, but what I've learned is, the biggest thing we ask them, to assess them, is, What do you do in your home time? Are you scripting on Python? Are you on a Metasploit? Are you coding? Are you taking raspberry pies and putting them together? Are you -- that's actually one of the best, most powerful assessment tools, so that's one of the things that we ask them, in terms of that.

And then, I think you've given us a lot of the powerful arrows in our quiver, which is to direct assess and direct commission. The Air Force has -- our -- in 15 days from now, our first two pilot direct commissionees go to OTS. One will be a second lieutenant, one will be a first lieutenant. So, we appreciate that.

We'll certainly get back to you on what we could ask of you in the next NDAA. But, I just wanted to offer the mission perspective as being the cornerstone for retention, from my perspective.

Senator McCaskill: Thank you.

Thank you, Mr. Chairman.

Senator Rounds: Thank you.

Senator Gillibrand.

Senator Gillibrand: Thank you, Mr. Chairman.

I just want to say, I agree with Senator McCaskill, strongly, that, please give us a request for authorities on any of the issues where you need support, resources, flexibility, whatever it is, any ideas.

[The information referred to follows:]

[SUBCOMMITTEE INSERT]

Senator Gillibrand: And I talked to Lieutenant General about this before. So, anything you need, we will provide, because we feel so passionately about this.

For Generals Nakasone and Weggeman, you're both building out Reserve components for cyber capability right now. The Guard has now built a new -- out -- Task Force Echo, which has been deployed to Fort Meade. General Nakasone, what do you see as the long-term mission of the Army Guard cyber component?

General Nakasone: Senator, reference our Guard component, we'll build 11 teams over the next 4 years. They will be doing both State missions, when not activated, and they will also -- doing such things as Task Force Echo, which is a mobilized mission to protect our infrastructure.

What we have found, working with the Guard, are several elements. First of all, incredible base of talent. Secondly is the ability to provide them the same training standard that our Active component gets. And the third thing is to equip them with the same tools that we use on the Active side and the Reserve side. That's powerful for us, ma'am.

Senator Gillibrand: And I think you agree with this, but could the Guard help address some of the existing gaps in our whole-of-nation approach to cyber? And could it serve as a conduit between State, local, and Federal

government, as well as the private sector, because of the unique relationships on the ground, and authorities?

General Nakasone: I do agree, Senator.

Senator Gillibrand: And, General Weggeman?

General Weggeman: Thank you, ma'am. Yes, I'll go first -- last question first.

So, absolutely. And I think the Air National Guard of the 262 Cyber Operations Squadron in Washington State is a great exemplar of how you can partner with State utilities, and now they're working through the legal dimension of even a private-sector utility, for how we would provide support from a -- an industrial base SCADA system support and electrical power SCADA system support. So, that's the Guard, the citizen airmen in that State, helping both their State and private-sector utilities. And that's actually ongoing. And they have three dedicated ten-person UTCs -- think of them as deployable teams -- that are specialized in EP, electrical power, SCADA systems, as one example to this. So, we're already -- I think that they're a great exemplar to go to.

In terms of, you know, the Air Force, we've built in, in our CMF build, Guard and Reserve capabilities already. So, right now we have 15 Guard cyber squadrons that have contributed to build three of the Active Duty CMF teams -- two cyber protection teams and one national mission team.

They're currently -- actually, the Guard forces from New York, New Jersey, and Texas are the three --

Senator Gillibrand: Great.

General Weggeman: -- States currently manning those teams. They've gone through ten full mobilization rotations. And so, in dwell right now, the Air Force already has ten cyber protection teams in the Guard in dwell for surge capacity, if required.

Senator Gillibrand: I'd like to ask you, for the record, both of you, for a -- recommendations in terms of how we could use the National Guard to support next year's election from cyberattack as a critical infrastructure. And I understand, from earlier hearings, that you don't feel you have that authority from the President. But, what I would like from this committee is recommendations to this committee that, if you were given that authority, what you would like to implement and what resources or support you would need to implement that specific mission. And I will then use that. Because this is something that both Senator Rounds and Nelson have been very focused on, because we do see the election as critical infrastructure. We do see an attack on our election infrastructure as a declaration of war. And I want to know, if we ever were able to give you the authority to protect the next election, how you would use the National Guard, specifically, to do that, and what

additional either resources or authorities you would need if you were tasked with that duty. Because that's something this committee has been very focused on for a long time, and we'd like your input, specifically, if we were to do that in the NDAA.

[The information referred to follows:]

[SUBCOMMITTEE INSERT]

General Weggeman: Okay. So, I appreciate, ma'am, giving the latitude that -- if the policy was given and the authorities were given, I think there's two specific things that I think are essential, and it kind of goes to the fire forces we've learned that can fight fires, and it goes to pre-scripted knowledge and missions. Unless you want us to be what I would call a "wet cleanup on aisle five force," if you want us to be there and preventatively build security --

Senator Gillibrand: Correct.

General Weggeman: -- and defense to thwart malicious cyberactivities, we would need the authorities and the tools and the infrastructure -- some of our defensive kits -- that are purposely tailored to the networks and systems that you would want us to support the State and local SCADA -- or, sorry, infrastructure CICR systems with. So, you know, we need to know the networked topology, we need to know the hardware, firmware, software that it operates so that we could be responsive, we could sensor, we could share information, and we could be proactive in defense.

Senator Gillibrand: So, that is the guidance I'd like you to write to this committee by letter to say, "If we were ever given this responsibility, if we were ever given this authority, these are the ten things we would need." And that's item number one. "We would need access to all the information and systems that are used, State by State. We

would need access to the resources to be able to develop expertise in each of these systems. We would need X, Y, and Z."

So, just tactically, what do you need? And then, we can at least, as a committee, decide, Do we want to put that in the NDAA as authorities for you to then go ahead and do? Obviously, the President would have to sign off on that. But, as our work from the committee, we've had so many hearings on cyber, specifically, and I feel like your hands have been tied every time we talk about one critical infrastructure, which is our electoral system. And we already know we have foreign adversaries who are hammering it daily. We also know that you -- that we now have the technology, because we had a hack-a-thon and actually effectively hacked vote totals. Our own cyber experts could do that within, I think, a 24-hour period. So, we know what the vulnerabilities are. I just want to proactively know from you guys, with your expertise, what you would need if I was -- if you were told you need to prevent this and you need to start a new mission.

General Weggeman: Yes, ma'am.

Senator Gillibrand: So, just guidance, so we know what it looks like. We also have several private-sector think tanks working on this, as well, what would be their recommendations to go to every one of the 50 Secretaries of

State. We'll have that information soon enough. We have a bill with -- Senator Graham and I -- to create a 9/11-style deep dive to assess what are the vulnerabilities and what are the ten things, as a secondary effort, too. But, in the meantime, I'd like your guidance, because if we can put it in the NDAA in April -- or, when is the -- it's soon. It'll be soon.

Senator Rounds: We're in the middle of it now.

Senator Gillibrand: Yeah, right now. So, it'll be soon when we get to vote on it.

Thank you.

Senator Rounds: Senator Nelson, I know that you're time-constrained, but if you'd like to make some comments or questions here, we'll do that before we start to finish up here a little bit.

Senator Nelson: Thanks.

General Nakasone, on the issue of direct commissioning, what are the legal limits that you cite? And should we alter them so that this program can be successful?

General Nakasone: Senator, what we are facing right now is an inability to grant constructive credit. As Admiral Gilday spoke to, constructive credit is the recognition of someone's abilities or experience in the civilian sector transformed and measured against what rank they may come in within the military. Right now, I believe

that we are limited to first lieutenant -- bringing them in as a first lieutenant. And so, we would like greater flexibility on that, based upon greater experience.

I think that's important when you think about some of the capabilities and some of the talent we're looking for -- people in big data, artificial intelligence, machine learning, forensics malware analysis. Those are all things that are not necessarily attractive to come in as a young first lieutenant.

Senator Nelson: And do you think that's hampering us getting people to join?

General Nakasone: I do, Senator.

Senator Nelson: So, how do you fix that? Put them at a higher rank?

General Nakasone: So, one of the things we've been working with your staffers is to look at how we better measure constructive credit to allow them to come in at a higher grade.

Senator Nelson: General Reynolds, tell me, if a -- if you get a direct commission into the Marine Corps, does that mean that they still have to be able to do 15 pull-ups?

General Reynolds: Yes, sir.

Senator Nelson: Good.

[Laughter.]

Senator Nelson: I'm glad, General.

Why should cyberspace be any different from other domains? Do we need the legislation to establish, without a doubt, that traditional military activities include cyber operations?

Well, General Nakasone, you're going to be the big chief --

[Laughter.]

Senator Nelson: -- so why don't you try to answer that.

General Nakasone: So, I don't think it should be any different than the other domains, Senator. I think that this has been a product of, you know, a very, very young and maturing force that we have, you know, some unique capabilities and characteristics of how we operate. Not having borders is something that, you know, really isn't applicable in the other domains, minus space. And so, one of the things that we, again, have come to is, you know, being able to define traditional military activities has sometimes been hard. It's much harder if you're not operating in this space. And now that we are continually operating in this space, I think we have a much greater way of being able to determine what traditional military activities are.

Senator Nelson: Thank you.

Senator Rounds: Admiral Gilday.

Senator Nelson: Sure.

Admiral Gilday: Briefly. Sir, I'm -- I respect your time, as you want to depart. The comment that I'd make with respect to cyber and traditional military activities is that the longer that it takes to integrate cyber into the other warfighting domains, the longer it takes to normalize it, the less -- the longer it takes for people to get comfortable with it, and the more it's treated as a special kind of action that it's difficult to get authorities for.

To the point that you made in your opening comments about the Russians -- and it's related to this -- we're at a point right now where we've allowed the Russians to establish those boundaries. We have allowed them -- in any other space -- the maritime, the air, the land -- you want to gain access so that you can dominate. You want to put the enemy -- you want to be in a position to dominate, whether it's physically or, in this case, virtually. The Russians, the Chinese, the North Koreans, when you talk about authorities, they have different rule sets, they have a lower threshold for aggression. And so, they are gaining the initiative. And so, it becomes more difficult for us to gain a position of advantage and to do the things that you want us to do.

Changing policy is one thing. The will to act is a completely different problem set that is just as important

as changing PPD-20 or changing any policies that underlie how we act in this space.

Senator Rounds: Thank you.

I'm going to follow up on this, because I think this really gets to the rut of a lot of the questions that you've heard today, and comments that you've heard today. I know that Senator Gillibrand has discussed the issue of the electoral process and how critical that is. But, I think you can look at almost any of our critical infrastructure right now and you can just simply ask the same question, and that is, If this was act of war or if this was an act of aggression using kinetic forces, whether by air, land, or sea, there would be an expectation by the American public that our defense forces would be in a position to respond, to defend. But, then also there would be an expectation that the deterrent forces would come to bear. Seems that with regard to cyber, we have yet to establish what those incidences are and at what point they reach the point to where there has to be a deterrent reaction on our part.

The Defense Science Board made it very clear that with -- for the next 10 years, our defensive capabilities will not be equal to the offensive capabilities of our peer competitors. It's become very clear -- and I think the discussion -- and, Admiral Gilday, I think you made mention to it -- Russia has a different norm, in terms of what they

see as the opportunities within the cyber domain. I think we've seen that with a number of the peer competitors and also some rogues, as well. And that is, is that they have used cyber as a way to impact our Nation's -- our assets -- in some cases, critical infrastructure and, in some cases, an electoral process. But, most certainly, they do it right now without a sense that we're prepared to offer that deterrence.

Can we talk a little bit about what it would take and about the challenges -- not so much -- and I recognize that this is an open session, but I think it's really important to lay out, you know, as I said, that -- when we talk about NATO issues and so forth, and we talk about international norms, there is Tallinn 1 and there is Tallinn 2.0, both of which try to establish what rises to an act of war in cyberspace and also what the incidences are that have to be responded to. Isn't it really true that, here, we have huge defensive capabilities, and that we have huge capabilities with regard to being able to infiltrate silently and gather a huge amount of data, as good as anybody in the world, and yet, at the same time, because we want to make sure that we follow the norms and that we are a respected neighbor, that we are very, very careful about how we respond in the domain of cyber? If it was air, land, or sea, there could be hell to pay, but in cyber we're not quite prepared to identify

and to state publicly what those norms are.

What are the policy discussions -- and if I had a group of enlisted men and women sitting in front of me right now who are on the front lines doing this, and it was in a classified setting, they would spill their guts about how frustrated they can be at times and what they would really love to be able to do, but they recognize their responsibility to adhere to clear policy choices.

And I know this is more of a statement than it is a question, but it's your turn now. You've thought about this a lot. Can you, in this open space, talk a little bit about the challenges that you see, and perhaps some of the frustrations that you have, in terms of protecting our critical infrastructure, civilian resources, and so forth, that perhaps the public simply doesn't recognize and that we should be talking about more?

General Nakasone: Senator, I'll begin on this. This is a very important question.

So, I think it begins with, What is the strategy for the defense of the Nation in cyberspace? That is an overall question that I think has to be asked, has to be debated, has to be discussed amongst policymakers, the American people, and others.

Senator Rounds: Would you -- let me just stop you right there. Fair to say that we really don't have a true

cyber policy established yet?

General Nakasone: So, I've learned, from my testimony over the past couple of weeks, Senator, that this committee has asked many times for a policy, and that one still has not been delivered. That's correct.

Senator Rounds: Okay.

General Nakasone: I would offer that, when we think about other defense of the Nation in cyberspace -- roles, responsibilities, functions, missions -- what are the elements that make it up? What are the parts of the government, what's the responsibility of the private sector that owns 90 percent of the networks that are necessary to protect?

The next thing I think about a lot is, What are the thresholds of support? So, when we think about this, how much of this responsibility should reside with the private sector, and at what point, when a nation-state actor has taken after our critical infrastructure, does it become the responsibility of the Department of Defense to defend the Nation? That is still a discussion point that I think is, you know, one to be had.

And so, those are just a couple, Senator, that I would offer as I've thought about this question over the past several months.

Senator Rounds: General Reynolds.

General Reynolds: Yes, sir. I'd like to just add one or two thoughts on this.

One of them is that -- I guess in my time in command at MARFORCYBER, going back to the Defense Science Board and what they learned about, you know, deterrence, one of the key findings was that we need to be able to deny the adversary. I don't want to speak for all of my peers here, sir, but we have spent an enormous amount of time even inside the service on this denial piece: How we make sure that what I own is defensible? And there was a lot of work to do. And so, moving forward, will we have additional capacity? Yes, sir, I think we would.

But, the other thing that I would like to make sure that we make a point here, in that -- and it goes back to the JTF Ares lessons learned. What Ares did, I think, for U.S. Cyber Command was provide a -- number one, a joint capability inside U.S. Cyber Command, so you have all the services represented there, but it also gave an opportunity for the combatant commands to reach into Cyber Command. In one single entry point, it gave the interagency one place, it gave our allies and partners one place to come in the counter-ISIL fight. And that was enormously important.

And so, I think, organizationally, moving forward, Who are the other combatant commanders that are involved in the plan against Russia? How are we organizing ourselves? It's

really essential, Senator.

Senator Rounds: Thank you.

General Gilday.

Admiral Gilday: Sure. Thanks for your question.

The main point that I want to make is that the force is not big enough, not based on the discussion that we had in this room this afternoon. If there's expectations to protect critical infrastructure, to hold significant adversaries at risk, adversaries that we are in contact with every day, then more needs to be done, in terms of the buildout and the development of a cyberforce that is comparable to the Nation's reliance on cyberspace for our economy, for our quality of life. It touches everything that we do. It's gigantic. And you take a look at the force, and you take a look at the number of trigger-pullers we have, 6,200 -- 6,200. Take a look at the United States Navy, take a look at the United States Army, take a look at the Marine Corps, the smallest of the services, and the Air Force, and make a comparison there. Based on what we talked about this afternoon in this room, the importance of cyberspace to the American people, to our quality of life, I think that that has to, at some point, be reassessed. And I think that the things that we have learned over the last 2 years need to play into that assessment. I think we need to be honest with ourselves. I think we need to act more

boldly.

Senator Rounds: General Weggeman.

General Weggeman: There's a benefit of going last. And I think a lot of the key points I would make -- to Admiral Gilday's last point, I agree. The scope and scale of CICR is extremely vast. And I agree, our force is too small. So, we will have to think deliberately and calculated, in terms of what would be DOD's role in -- to support that, and how do we best use a high-demand, low-density force, if a policy is written to where we would provide that, above and beyond the National Guard or the Reserves?

You know, so, as the former J5 at Cyber Command, I've been thinking about, you know, the cyber deterrence question for a long time. And I'll give you, simplistically, my frame.

The first thing is, the phrase is flawed. I believe the proper way to say it is "cyber indeterrence." Cyber -- it's -- what is cyberspace operations' role, offense and defense, in a national strategic deterrence campaign? Admiral Rogers testified that, you know, sometimes you don't want to use cyber when you come back. So, it's got to be a whole-of-government, if not whole-of-nation, campaign.

The second thing about any in deterrence is, Deter what? And I think what we constantly come back to in this

forum is, we want to say we want to deter malicious cyber activity. So, if we want to deter or erode an enemy's confidence in their ability to pitch malicious cyber activity at us, again, we need to use every arrow in our quiver as a nation to deter that activity. And we are but one. We may be the least -- have the least amount of capability or capacity. And so, we have to go to other things. But, I do think it's all about "cyber indeterrence," and that's really important.

I go back to the classic principles of, you know, within cyber we have to be able to impose cost, we have to be able to deny benefit, and maybe we do one in the cyberspace domain and other in another domain, whether it's land, sea, maritime, information, leveraging State Department or FBI or other agency partners.

And the last is the concept of -- in the Defense Science Board study, everything is about taking that first hit. It's a constant thing. For those of us who have been around, this is an offense-dominant domain. Our adversaries have exquisite capabilities. And if you want to be that second-strike force, you may not have that luxury. It's hard to recover. And so, I think we have to do a hard look at a nation, given the exquisite insights that our intelligence community can generate, the exquisite insights that our cyber forces and operators can generate. What is

the -- what is our realm of strategic preemption? And when would we have thresholds or triggers where we would strategically preempt a large release of malware that would take us down and set us back on our feet for a year?

Senator Rounds: Thank you.

Now, let me just finish with this. General Nakasone, the Ares project, they pointed out earlier that there were some challenges there, and that some of the conditions weren't the best. And yet, unless we clearly look at and we -- we're critical in the way that we analyze our successes and where we need to improve, we're not really doing our job. And so, the fact that we could have a frank discussion about improvements and so forth, that's a positive thing. And showing how far we've come in a very short period of time with regard to this particular domain, I think, is critical in creating more successful opportunities in the future. And if we ever get to the point where we can't look at those criticisms and say, "These are learning experiences, and we can do better, and we will learn from them," then we're in real trouble.

So, I -- first of all, I don't take offense from someone suggesting that there were challenges with a program and that we're going to have to do better in the future. And I think that's the way that it was perceived by the panel that's before us today. And I appreciate that.

Second of all, I think what we've talked about here today, while we're talking about the positioning, the capabilities of our forces today from your perspective, I think what you've given us, in terms of an insight as far as what the policy issues are and the understanding of the American public with regard to your mission right now and the role that you have been asked to play, versus what I think in many cases is the expectation of an American public that says, to begin with, "If someone attacks us in cyberspace, we should hit them hard in cyberspace" versus -- the appropriate role is -- just because someone attacks us by sea doesn't mean we necessarily have to attack only by sea. We can attack in a whole lot of different domains. But, it does require this, that unless we are dominant in air, land, sea, space, and cyber, our adversaries will take advantage of any opening they see.

And so, with that, I want to say thank you to Senator Gillibrand for being able to attend with us again today. I want to thank all of our witnesses here today for your testimony. This is not the last that we will see you all in front of our committees again.

And, General Nakasone, we look forward to visiting with you in a new role, as well, when the opportunity comes.

And unless any one of our witnesses has anything further to add, we will call an adjournment to this meeting

at this time.

Thank you.

[Whereupon, at 3:49 p.m., the hearing was adjourned.]