[H.A.S.C. No. 115–95]

CYBER OPERATIONS TODAY: PREPARING FOR 21ST CENTURY CHALLENGES IN AN INFORMATION–ENABLED SOCIETY

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

HEARING HELD
APRIL 11, 2018

U.S. GOVERNMENT PUBLISHING OFFICE
30–569 WASHINGTON : 2019

COMMITTEE ON ARMED SERVICES

ONE HUNDRED FIFTEENTH CONGRESS

WILLIAM M. "MAC" THORNBERRY, Texas, *Chairman*

WALTER B. JONES, North Carolina
JOE WILSON, South Carolina
FRANK A. LOBIONDO, New Jersey
ROB BISHOP, Utah
MICHAEL R. TURNER, Ohio
MIKE ROGERS, Alabama
BILL SHUSTER, Pennsylvania
K. MICHAEL CONAWAY, Texas
DOUG LAMBORN, Colorado
ROBERT J. WITTMAN, Virginia
DUNCAN HUNTER, California
MIKE COFFMAN, Colorado
VICKY HARTZLER, Missouri
AUSTIN SCOTT, Georgia
MO BROOKS, Alabama
PAUL COOK, California
JIM BRIDENSTINE, Oklahoma
BRAD R. WENSTRUP, Ohio
BRADLEY BYRNE, Alabama
SAM GRAVES, Missouri
ELISE M. STEFANIK, New York
MARTHA MCSALLY, Arizona
STEPHEN KNIGHT, California
STEVE RUSSELL, Oklahoma
SCOTT DESJARLAIS, Tennessee
RALPH LEE ABRAHAM, Louisiana
TRENT KELLY, Mississippi
MIKE GALLAGHER, Wisconsin
MATT GAETZ, Florida
DON BACON, Nebraska
JIM BANKS, Indiana
LIZ CHENEY, Wyoming
JODY B. HICE, Georgia

ADAM SMITH, Washington
ROBERT A. BRADY, Pennsylvania
SUSAN A. DAVIS, California
JAMES R. LANGEVIN, Rhode Island
RICK LARSEN, Washington
JIM COOPER, Tennessee
MADELEINE Z. BORDALLO, Guam
JOE COURTNEY, Connecticut
NIKI TSONGAS, Massachusetts
JOHN GARAMENDI, California
JACKIE SPEIER, California
MARC A. VEASEY, Texas
TULSI GABBARD, Hawaii
BETO O'ROURKE, Texas
DONALD NORCROSS, New Jersey
RUBEN GALLEGO, Arizona
SETH MOULTON, Massachusetts
COLLEEN HANABUSA, Hawaii
CAROL SHEA–PORTER, New Hampshire
JACKY ROSEN, Nevada
A. DONALD MCEACHIN, Virginia
SALUD O. CARBAJAL, California
ANTHONY G. BROWN, Maryland
STEPHANIE N. MURPHY, Florida
RO KHANNA, California
TOM O'HALLERAN, Arizona
THOMAS R. SUOZZI, New York
JIMMY PANETTA, California

JEN STEWART, *Staff Director*
PETE VILLANO, *Professional Staff Member*
LINDSAY KAVANAUGH, *Professional Staff Member*
NEVADA SCHADLER, *Clerk*

CONTENTS

CYBER OPERATIONS TODAY: PREPARING FOR 21ST CENTURY CHALLENGES IN AN INFORMATION–ENABLED SOCIETY

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
Washington, DC, Wednesday, April 11, 2018.

The committee met, pursuant to call, at 10:02 a.m., in Room 2118, Rayburn House Office Building, Hon. William M. "Mac" Thornberry (chairman of the committee) presiding.

OPENING STATEMENT OF HON. WILLIAM M. "MAC" THORNBERRY, A REPRESENTATIVE FROM TEXAS, CHAIRMAN, COMMITTEE ON ARMED SERVICES

The CHAIRMAN. Committee will come to order. Looking back at my notes from 10 years ago, when Mr. Smith chaired what is now the Emerging Threats and Capabilities Subcommittee and I was a ranking member, I found a number of references to preparing for cyber as a new domain of warfare.

This committee has held many hearings and briefings on this topic over the last decade, and we are continuing with more this week, led by Chairwoman Stefanik and Ranking Member Langevin.

We have also enacted a number of legislative provisions and authorized a lot of funding, and there's no doubt a lot of it—progress has been made in building up our military and intelligence capabilities in cyberspace.

But I do not think it is an exaggeration to say that our Nation has still not faced up to the threat. Cybersecurity means lots of things. Part of what it means is going on down the hall in another hearing, but part of it is what we are going to talk about today.

Threats to national security in cyberspace come from adversaries stealing information. Sometimes it comes from adversaries working to manipulate our decisions and American public opinion. Part of it is the potential to disrupt our economy and unleash havoc with our financial system, or electric grid, or public health and sanitation. And I have not even begun to discuss the consequences for the effects of our military's ability to operate.

We still have not answered the fundamental question of what we expect the Federal Government to do to defend our citizens, our businesses, our infrastructure, and our society in cyber. Meanwhile, the capabilities of our adversaries and their willingness to use them is growing far faster than our response.

The Director of National Intelligence [DNI] recently assessed, quote, "the potential for surprise in the cyber realm will increase in the next year and beyond as billions more digital devices are

connected—with relatively little built-in security—and both nation states and malign actors become more emboldened and better equipped in the use of increasingly widespread cyber toolkits."

Fortunately, our witnesses today have a lot of experience and a lot of expertise in these issues, and I am grateful to each of them for their willingness to share their views today, in the hopes that, not just our committee, but the Congress and the country can move at the appropriate pace in confronting these challenges.

Mr. Smith.

STATEMENT OF HON. ADAM SMITH, A REPRESENTATIVE FROM WASHINGTON, RANKING MEMBER, COMMITTEE ON ARMED SERVICES

Mr. SMITH. Thank you, Mr. Chairman. I agree completely with the chairman's opening remarks and will not repeat them. We all know the importance of cybersecurity; I think the chairman outlined it very well.

And the challenges that I am most interested in hearing from the three of you on, and in—we have all been people that have been working on this for a long time, is number one, how can we better coordinate the effort? Is—it's, you know, a thousand points of failure and then some when it comes to cybersecurity.

And within DOD [Department of Defense] alone—I mean, forget about the contractors and all the other pieces of our cyber network that are vulnerable to attack. Within DOD, I still don't think it's clear who's in charge. I don't think it's clear what the strategy is, and I don't think all the key components at DOD have any idea of really exactly what—what the plan is. Or, overstatement, say "no idea," but they don't have a clear plan.

So how can we develop that agenda so that within DOD we have people who are clearly in charge, and we say, okay, what is going on in cyber? This is the chain of command. And this is what is going on with it, and how we would respond to it.

Second, I would—do want to emphasize one point the chairman made, and that is, when it comes to information campaigns and disinformation campaigns, cyber has taken these to a whole new level. And I guess one of my frustrations is while it's taken to a whole new level, on the one hand, on the other hand, it's nothing new. I mean, the medium is new.

Disinformation, information, whether it's, you know, through the radio, or newspapers, or whatever the medium of the time was, you know, we have been doing that since the beginning of this country. And yet we seem to be unbelievably slow to respond to using this new tool, this new medium, for spreading the story that we want to spread, whereas in contrast certainly Russia, but I also think China, have been incredibly aggressive and are unquestionably ahead of us in using this technology. How do we catch up?

And the last thing—great debate about storing information in the cloud, using open source software versus closed source software, and I have had a number of very, very smart people from out in Seattle passionately argue to me that we can better deal with cyber—the more stuff we have in the cloud and the more we rely on open source software, that it is a better—you can better protect that type of software.

So I am curious what your guys' thoughts are on the cloud and open source and how it fits into us developing that cyber strategy that we so desperately need.

And with that, I yield back. Thank you, Mr. Chairman.

The CHAIRMAN. We are pleased to welcome the Honorable Michael Chertoff, Co-Founder and Executive Chairman of The Chertoff Group and of course also former Secretary of Homeland Security.

General Keith Alexander, Founder and Chief Executive Officer of IronNet Cybersecurity, former Director of the National Security Agency.

And the Honorable Jeh Johnson, partner, Paul, Weiss, Rifkind, Wharton & Garrison, but also former Secretary of Homeland Security, and General Counsel to the Department of Defense, which may play a role here.

Without objection, each of your written statements will be made part of the record, and we would be pleased to hear whatever oral comments you would like to make at this point.

Secretary Chertoff.

STATEMENT OF HON. MICHAEL CHERTOFF, CO–FOUNDER AND EXECUTIVE CHAIRMAN, THE CHERTOFF GROUP

Mr. CHERTOFF. Thank you, Mr. Chairman, and thank you, Ranking Member Smith. I appreciate the opportunity to testify. I thought I had testified before pretty much every committee in Congress, but I hadn't before this one. So you have moved me towards a perfect record, or a royal flush.

I think this is a very timely hearing, and maybe not quite as well attended as the one down the hall, but in many ways I think focusing on an area that requires greater attention, and I think that the opening remarks, I think, make that point very well.

Let me just very briefly summarize a couple of points. First of all, there's no question in my mind the threats have increased in intensity and frequency. We now are dealing with what I would call industrial-scale data theft, whether it is the billions of accounts on Yahoo that were stolen, or the OPM [Office of Personnel Management] hack, which resulted in north of 20 million very sensitive files being taken.

I mean, this is really theft on an industrial scale, and it applies to straight-out criminality, as well as to things that are relevant for intelligence purposes.

We have seen what we call information operations, the use of cyber means, including hacking, to disseminate data which is part of an attempt to influence and disrupt our elections and our democracy.

We have seen data destruction with ransomware—WannaCry, NotPetya—which has had a serious impact on civilian infrastructure in various parts of the world, including some major enterprises.

And as was recently announced by DHS [Department of Homeland Security], we have found malware in much of our critical infrastructure, including our electric grid, and if you go back and look at the Ukraine in 2016 and 2017, Christmastime, the lights went

out because of cyberattacks that were mounted against the electric infrastructure there.

So there's no question whether it's theft of data or information, or actually disruptive or destructive attacks. We have seen an increase in severity and frequency.

And I want to be clear by defining a couple of things. First, when we talk about protecting the data, we are talking about protecting confidentiality, availability, and integrity. And that is different than the issue of the content itself.

And I say that because I know the Russians have a concept of what they call information security, which to them means, let's keep information we don't like off the network. We call that censorship in this country, and it's important not to confuse the two, because what we want to do to defend the availability, confidentiality, and integrity of data is a different set of considerations than when we deal with the issue of content that we happen to disagree with.

So with that being said, let me briefly just summarize a couple of points. First, as it relates to defense, I do think we have made some progress on unity of effort with the U.S. Government, but not as much as we need. In theory, the major agencies that deal with cyber—the Department of Defense, Homeland Security, and the FBI [Federal Bureau of Investigation]—have distinct roles, and when you have a lead role of one, for example, in a particular area, and the others support, but we need to make sure we exercise that and institutionalize it.

As far as the private sector is concerned, there we have the challenges—you have got widely distributed ownership and control of infrastructure, and uneven capabilities and knowledge about how to defend that infrastructure.

Some of the things we can do to make that a little bit easier are continuing to promote information sharing, particularly having it be automated, and having the ability to use a common language to describe threats, and I would argue also being—making clearances a little bit more widely available to the private sector so that there could be greater in-depth sharing of information.

I think the propagation of additional standards about what are considered to be good cyber defense measures will be helpful to the private sector. And I would also urge Congress look at the SAFETY [Support Anti-terrorism by Fostering Effective Technologies] Act, which has worked well in promoting counterterrorism technologies, as perhaps legislation that could be extended to counter cyber-attacking technologies, and that again would incentivize the private sector to invest in better cyber defense.

And the last area I would look at would be the so-called "internet of things." We are seeing a dramatic expanse—expansion of the surface area of attacks through so-called "smart objects" that have very little provision for security or cyber defense, including basic things like patching and upgrading. And we may need to look at some legal regulations or policies that would promote some kind of at least minimal integration or security capabilities into these increasingly widespread smart devices.

Finally, on the issue of what we might do in terms of either active defense or offense, I would argue that there are a couple of

areas we should look at. And I don't think it's a capabilities issue as much as it is a policy and strategy issue.

First, we need to be clear about standards for attribution. What do we expect in terms of the standard that we must meet to be confident about our attribution, and how would we announce to the world that we have made—we have attributed something in a way that we want to respond to?

Second, I think we need to marshal all of the tools in the toolbox in terms of response. It can't only be cyber response. Depending on the nature of the attack, it has to be potentially criminal, a prosecution, the use of sanctions, and even the use of cyber and physical tools to preempt something in an appropriate case, when we are dealing with something that threatens life or property.

And finally, a couple of other areas where I think we need to focus on international responses. One is coordinating with our—our allies in NATO [North Atlantic Treaty Organization], in terms of having a common doctrine and a common set of capabilities in cyber response, and then looking to creating a more robust set of international norms and rules about what is off-limits in cyberspace as it is in physical space.

Because right now, we are not always clear about what ought to be considered to be illegal cyber activity under international law, and I think the time for some kind of a set of norms and laws in this respect is well overdue.

So with that, Mr. Chairman and Ranking Member, thank you very much, and I will be pleased to answer questions.

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

The CHAIRMAN. Thank you.

General Alexander.

STATEMENT OF GEN KEITH ALEXANDER, USA (RET.), FOUNDER AND CHIEF EXECUTIVE OFFICER, IRONNET CYBERSECURITY

General ALEXANDER. Mr. Chairman, Ranking Member Smith, distinguished members of the committee, it's an honor and privilege to be back here again. I want to hit, over the next 2 hours, no, the next 5 minutes, five key points.

First, technology. You both mentioned it. We live in exponential times. The amount of applications, the amount of data, and the amount of technology is growing—almost doubling every year in each category. That means cyber is going to grow exponentially, and the problems that we have today, a year from now, will be more than twice as large.

The threats are growing with that. And nation-states are now using cyber as an element of national power, not only to—from a criminal perspective, for stealing money and intellectual property, but now to impact other nation-states. We see it in Ukraine, you saw it in Georgia, you saw it in Estonia. You see it now in the Middle East, in Kuwait, Bahrain, UAE [United Arab Emirates], Qatar, in Saudi Arabia, and you see it in Japan and Taiwan, and South Korea.

Countries are being hit with nation-state attacks, and we expect, we should expect, that those countries we have disagreements with will use cyber to attack us. And we are not ready.

And the reason we are not ready is not because there aren't good people in government working hard, it's because, in my opinion, we don't have the policies in place, we don't understand the roles and responsibilities sufficiently between the departments, and we don't train between government and industry.

Let me give you a few examples of what I think we need to do, and why we need to do it. And then I will end up with four key points that I think, as a government, we need to go forward on.

With respect to the roles of government, it's clear, I think, the missions of the Department of Homeland Security for incident response, for setting standards, it is clear for the Department of Justice what the FBI does in terms of law enforcement, and clear in the mission of the Defense Department to defend the Nation from cyberattacks, especially from nation-states.

The problem. Government, one, can't see what is going on in cyberspace like we can in an integrated air defense system. You can't see it, and so most of our response is incident response and falls on the Department of Homeland Security, who—who leverages everything from the other departments have—to help do that.

But that's not what our Nation needs. If you go out and talk to companies that have been attacked, they don't want you to come and tell you they have been attacked, they want help in stopping the attack. And to—to date, most people say it's too hard. In the Constitution it says our government is here for the common defense. It doesn't say we are here for the common defense unless it's hard, we are here for the common defense unless it's fast, or we are here in the common defense unless it's in cyber. Our job, your job, is how we defend this country. And I believe it is doable.

And the issue gets back to some of the things that you mention about the cloud. How do we leverage the cloud for pushing up a common picture in cyber where malicious acts are going. Technically achievable. And we need to drive towards a solution like that, that brings together our government players in a coherent, policy-provided path that allows our government to work with industry to actually defend this Nation. And I think it's doable.

In my experience in talking to industry is they are—they are more than willing, and we have given them the authority to share the necessary information with government under the CISA [Cybersecurity Information Sharing] Act. We now need to make that real.

But there are still several things that I think limit that sharing. One of them is liability protection and the concerns of liability. For small and midsized companies, how do we incentivize them to actually have good cyber and the ability to share real-time information? How do we share this information in a credible way, and make sure that the information flow that goes back and forth between government and industry is there? And that may require, as Secretary Chertoff said, clearances from many of those in industry.

Let me give you one set of examples about how we could defend this country. Today, if a bad actor—so, in running Cyber Command [CYBERCOM], we would look at how the threat looks at attacking

our Nation. They don't look at it by company. They look at it by the effects they want to do to hurt our country. That means the energy sector, the finance sector, the healthcare sector, and the government.

And what they do is they look for weak spots, they get in, and then they can cause damage from there. But we look at defending at a point, not collectively across sectors. So we now have to look at our Nation, and use cyber in a networked way, just like we have the internet, so that we can defend it at network speed.

And I put that last part in there—it has to be—information sharing has to be at network speed if you want to stop the threat. And I believe that is viable and doable today, and something that we should collectively push for.

Thank you very much, Mr. Chairman.

[The prepared statement of General Alexander can be found in the Appendix on page 57.]

The CHAIRMAN. Thank you. Secretary Johnson.

STATEMENT OF HON. JEH JOHNSON, PARTNER, PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP

Mr. JOHNSON. Mr. Chairman, Ranking Member Smith, members of this committee, it is a pleasure to return to the House Armed Services Committee. When I was General Counsel of the Department of Defense, I testified several times before this committee in the years 2009 to 2012. While I was Secretary of Homeland Security, I had the pleasure of testifying before Congress 26 times in 37 months, and since I have been a private citizen now for 14 months, I have testified—this will be my third time.

As Senator Angus King said to me last month, when I testified before the Senate Intel [Intelligence] Committee, "Mr. Secretary, how can I miss you if you never go away?" And he is right. And one of these days, I do expect to go away, but I welcome the opportunity to come here and testify with my two friends and colleagues on this important topic.

You have my prepared statement, in which I tried to describe the range of cybersecurity threats that I see, ranging from those that this committee is well acquainted with, the prospect of a nation-state cyberattack on our critical infrastructure, to the issue that the witness down the hall is probably testifying about, the inappropriate or unauthorized use of private data that American citizens make available on the internet.

In my testimony, I also take on the legal question that many ask: what type of cyberattack may constitute an act of war? And I will be happy to answer questions along those lines, if the committee members have it. In general, I look forward to our discussion, and I am pleased to be here with General Alexander and Secretary Chertoff. Thank you.

[The prepared statement of Mr. Johnson can be found in the Appendix on page 68.]

The CHAIRMAN. Let me just ask each of you to respond to kind of two high-level questions, I guess. One is, my perception is the threat is going up far faster than our response. We are getting more capable, but as at least a couple of you mentioned, our pol-

icy's not there. Do you agree with me, is the question, that the threat is growing faster than our response?

And the second question is—and I will broaden this to Congress—if you could wave a magic wand and have Congress do one thing this year in this area of cybersecurity, what would you like to see us do?

Mr. CHERTOFF. I guess I will begin. I think the answer to the first question is I agree with you. I think the threat is increasing. I think, again, it's not a—on our side, an issue with lack of capability, I think it is that we haven't firmed up a doctrine and a strategy for how to respond.

We are beginning to see some response. I mean, I think for example in the criminal side you are seeing some indictments. I think sanctions are a potential response. There may be things going on below the surface that are not—not visible. But there's no question that the threat is intensifying, and the boldness of the bad actors is intensifying.

In terms of what Congress can do, I think on the issues of strategy and doctrine, these are—are I think matters really more for study than for some specific legislation.

But I come back to the SAFETY Act. I think in dealing with the private sector, one of the issues I hear a lot is, "Well, how much do we invest, and what is the return on investment in terms of cybersecurity?" And one thing that I think was demonstrated in the counterterrorism area was the SAFETY Act really incentivized the private sector to invest in tools that could be used to counter terrorism. Because there was a liability protection that came with it.

And I think extending that to cyber would be a very easy, straightforward thing that would begin to create some incentives for the private sector.

General ALEXANDER. So I think, yes, the threat is going up exponentially, and technology is fueling that. So, consider that they are getting more opportunities and going faster than our policy and doctrine is growing, so we are falling behind.

And if I were to give you one thing—I liked yours, so I will add to—a slightly different—we don't have a common operating picture for cyber. We can't see, as a Nation, other nations attacking us. As a consequence, we have limited abilities to actually defend our Nation at network speed, which is what will be required, I think, in the next few years.

So one thing, if you could push to build a common operating picture for government and industry for attacks that are hitting our country.

Mr. JOHNSON. Mr. Chairman, I agree with your assessment that the cyber threat to our country is getting worse. I believe it will get worse before it gets better, and I believe those of us on defense struggle to keep up. I think that bad cyber actors, ranging from nation-states, to criminals, to "hacktivists," to those who engage in ransomware are becoming increasingly aggressive, creative, and tenacious.

If I had a magic wand, and if I were Congress—or, I would say a Congress of one—I would in some way—and politically, this is very challenging, but in some way find a way to either regulate or

encourage those in the private sector to embrace certain minimum cybersecurity standards.

I note that the Senate Intel Committee report on election cybersecurity encourages voluntary compliance with certain minimum cybersecurity standards, but I think that that's a commonsense solution to a lot of our problems here, and we don't have that right now.

The CHAIRMAN. Let me pose one other brief question to General Alexander and Secretary Johnson on the Department of Defense in particular. I pick up frustration with some of our military folks that they are being held back from being able to use cyber tools to the extent they think makes sense.

And I know there's a number of challenges. Using cyber tools may lose you intelligence-gathering capability, all sorts of difficult legal issues, and we don't have time at this point to go into all of that.

But I am just wondering if either of you-all have an opinion about whether, for the military use of cyber to create certain effects, are we moving at an appropriate pace, or are we too hesitant to give, say, our combatant commanders and other military leaders the tools that we could give them, but because this is new and difficult, we are reluctant to do so?

Mr. JOHNSON. Mr. Chairman, I think that the perception you have detected is probably accurate. Among our military cybersecurity personnel, without getting into too much detail, I know that some feel that the law and traditional law of armed conflict principles, traditional international law principles, restrain our ability to use some of our current capabilities.

And so I share your perception.

General ALEXANDER. Mr. Chairman, I think what is lacking in that regard is rules of engagement. So you have U.S. Cyber Command, who has the responsibility to defend the Nation, and the issue really comes down to when do you fire back, and what authorities do you need to get before you fire back to defend the country?

Most of the time, it would be up to the commander of Cyber Command to do it and ask forgiveness. That's not a good place to put a military person in. You need rules of engagement that say, "If I see an attack that is going to destroy our energy sector, our finance sector, or something, and I have got 60 seconds to act," you want that person to do the right thing. You need to give them rules of engagement, and get the government to agree, and you all to agree to those, and then train to them.

And that's something I think that's sorely lacking, at least when I was commander of Cyber Command.

The CHAIRMAN. Okay, thank you. Mr. Smith.

Mr. SMITH. Thank you. We have talked a little bit about the sort of rules of engagement. I think this is one thing that is a significant problem is our adversaries feel like they can operate, to a certain degree, with impunity, because we have not made clear how to respond.

What I would like from you—and I will get a little bit more of a preview of this is—what would that look like? If you said if you were God, you know, what would you say what should our rules

of engagement be? You know, some have said that, you know, a cyberattack is an act of war—I don't want to go there.

I don't think that a cyberattack is equivalent to 9/11, or equivalent to if, you know, Russia or anyone else were to launch missiles at us. I don't—I don't believe that if we suffer a cyberattack, we should start bombing whoever it is we think attacked us.

What would be an appropriate response, so that people felt like there was a price to pay if they continued to attack us through cyber? And they—they could do a lot worse than they have done, but they—there certainly have been—you know, even as we sit here, I am sure there are cyberattacks going on. No one knows what the consequences are. What should they be?

General ALEXANDER. So I will give you my thoughts——

Mr. SMITH. Sure.

General ALEXANDER [continuing]. On responding to an attack against the country, and I will use the 2012 attacks that occurred. And in those time, it was my experience that the attacks that were coming against our country could have been stopped and turned off, not destructive attacks, but blocking attacks. But some of those blocking attacks would be in foreign space. So that creates the norms that Secretary Chertoff brought up, and some of the issues.

Now, interestingly, most of those systems that are being attacked have been exploited by a bad guy to attack us. So the country that's—whose device—computer sits in their turf is actually being used to shoot us. In physical space, if somebody put a weapon in neutral space and started shooting at you, you have the right—inherent right for self-defense. I think we need a similar thing in cyber, where you can defend it.

Now, the administration needs, beyond the blocking mechanism—so, my rules of engagement aren't to go out and try to take out a country, it would be stop it, give the administration the opportunity to think of what elements of national power they want to use to counter it, and that could be diplomatic all the way to the military.

But what—what you are asking, and the Cyber Command forces to do, is block that attack and give you the time you need to make a decision on what elements of national power.

Mr. SMITH. I guess one sub-question on that: How easy is it to know where the attack is coming from? This is a matter of no—no small importance, given our current debate about Russia and what they are doing to elections and everything, you know, you—you have sat there, and you have—you have looked at that, so all of you have.

Is it really true that sometimes you can't tell, or are you pretty confident from your position that after a few hours that you know where it's coming from?

General ALEXANDER. I think our attribution improved immensely. And you would have to ask them where they are today, but from 2005 to 2014, it was significant growth in attribution at network speed. The issue may not be that you have it down 100 percent of which element in a country is doing it——

Mr. SMITH. Right.

General ALEXANDER. But for the picture that I talked about, if you had that picture, it becomes increasingly clear. And the intel-

ligence agencies can provide the rest of the picture if you give them the information at network speed. So hopping through a number of channels, what you need to do is see those at network speed. You can see how that plays out, and pinpoint where it goes back.

Mr. SMITH. The bottom line is we ought—we ought to be able to do it, so then we can have the—that's once we figure out what the appropriate response is to this, at least we know who to send it to. Do either of you——

Mr. CHERTOFF. I would just—I would add just a couple of elements to this. First of all, on the issue of attribution, the challenge is not only to determine which is the server from which the attack originates, but to what extent you can—you can——

Mr. SMITH. Who did it?

Mr. CHERTOFF [continuing]. You can pin that on a—on a government agency. And one thing we have seen the Russians do is create a deniability situation with criminal groups, where the—essentially, the argument is as long as you don't commit crimes in Russia, you—feel free to go and do whatever you have to do overseas, but when we call on you, you will help us get into something. So that gets into a legal issue about how we hold countries accountable when they provide tacit encouragement.

The second issue, which is challenging, is unlike in the—in the physical world, where you could see a missile or a bomber coming from overseas, you could easily have a nation-state attack launched from a café down the street here in Washington from a thumb drive. We have built our doctrine in terms of what the military can do, and in terms of the away game and the home game, and we may need to revisit when we use some of our away powers for attacks that emanate from home.

Mr. SMITH. I want to let some other people get in here, so just very, very quickly, how does the DOD's plan to move into the cloud and more use of open source software impact cybersecurity? If you can give me, like, just 30 seconds apiece on—because that's the direction we are heading in. How does that impact our ability to protect ourselves?

General ALEXANDER. I think by and large it's a good thing. We need to do that to get the collective picture. So going there, I think you can provide the security—the secure web gateways and stuff that are coming in, the tools that are going—I think it provides better security. You alluded to that, and I think you are correct.

It's more—it's easier to do it in that way. You just make it—need to make sure you have the resilience.

Mr. SMITH. Okay. Anybody else want to comment on that? Okay. Thank you very much, Mr. Chairman, I yield back.

The CHAIRMAN. Mr. Wilson.

Mr. WILSON. Thanks, Mr. Chairman, and thank each of you for being here today, and your obvious many years of service to our country and dedication to the American people. And I want to begin by thanking Chairman Mac Thornberry for this very important hearing, as I believe that information warfare will expand beyond the current and future battlefield.

I would also like to thank and congratulate Chairwoman Elise Stefanik for her leadership on the Emerging Threats and Capabili-

ties Subcommittee, advancing American interests in cybersecurity to protect American families.

A concern that I have in—General, you actually brought it up, and then you have all touched on it, but it's so critical and that is how do U.S. agencies conduct a measure of cyberattack? Do all agencies share a common metric to measure a cyber incident?

Last year, I introduced H.R. 1030, the Cyber Attack Standards of Measurement Study Act, which would require the Director of National Intelligence, in consultation with the Secretary of Homeland Security, the Director of the FBI, and the Secretary of Defense, to conduct a study to determine appropriate standards to measure the damage of cyber incidents for the purposes of determining the response to such incidences, and to include a method for quantifying the damage.

And General, beginning with you, but actually all three of you, I would like to know: Do you believe that we—having a common interagency metric for measuring a cyberattack would benefit the coordination of a response? And then secondly, should there be an appropriate counter response to whoever conducts the attack?

General.

General ALEXANDER. I have some out of bounds thinking here in terms of DHS, but yes, I think you ought to do standards. I think I would take it one step further. I think the Department of Homeland Security, with what they are running in the NPPD [National Protection and Programs Directorate], and where they have the security operations centers, should actually provide for the common defense for the rest of government and the ability to do it.

I don't think the smaller government agencies have the technology and the people to do that. I would consolidate that, just as business does, and give that authority there. I think that would help in what you are trying to do.

Mr. JOHNSON. Congressman, I think that the legislation you cited sounds like a good idea to me. I would be careful, though, that in terms of trying to measure the effects of a cyberattack, it's not necessarily one-size-fits-all, because you are assessing, say, the theft of personnel security records, versus the theft of something in the Department of Defense.

And I endorse what General Alexander said, that there are smaller Federal agencies that are simply not equipped, and need the Department of Homeland Security for a lot of help in this area.

Mr. CHERTOFF. And I am in complete agreement with that suggestion as well.

Mr. WILSON. Thank you, again, and it is really just so frustrating to think of how blatant the attacks on American citizens, our government, our businesses—but not just us, as we see our allies in the Baltic States, or our allies in Korea, in Japan.

Another concern I have is with attribution. We have a significant and persistent obstacle in—facing our ability to respond. Do you believe that state actors—and again, General, you get stuck with this first, okay? But that state actors such as China and Russia take advantage of vulnerabilities in our ability to legally attribute a cyberattack.

What can Congress do to address this issue of attribution?

General ALEXANDER. Well, I think, first—and Secretary Chertoff made a comment on the attribution, and I would just agree with that. That's very difficult. Something that we need to work, and I believe Russia and China use forces that they can push out there to go after us, which makes this very hard.

I don't know the best legal way to do it, but I think that's a discussion that has to be had as a Nation. I think we are going to see that—and you have mentioned the Baltic States, Eastern Europe, and we are going to see it in the Middle East, and I believe with events going on in Syria and elsewhere, it's going to hit our country. So we need to get out in front of that.

Mr. CHERTOFF. I mean, I agree with what General Alexander said. Look, the challenge with attribution I don't think is so much a technical challenge as a decision we have to make about, A, the level of certainty we need for certain kinds of responses, and B, the extent to which we are prepared to publicly reveal why we make a certain attribution.

So we have seen lately, for example, the Department of Justice charged a couple of FSB [Federal Security Service] Russian intelligence agents in the case involving the Yahoo hack. That's a good thing. I think sanctions can be a better thing.

Now, if we were to get into something that was really seriously destructive, with a loss of life, such that it might warrant a response at the level of warfare, then we might want a higher standard. I would rather have that discussion, at least quietly, now, than try to figure it out when we are in the middle of an attack.

Mr. WILSON. Thank you very much. And Secretary Johnson, I look forward to getting with you later. Thank you.

The CHAIRMAN. Ms. Davis.

Mrs. DAVIS. Thank you, Mr. Chairman, and thank you to all of you for being here. Along with the—the discussion that we were just having, little bit about IP [intellectual property] abuse, and we know how destructive that can be. And what is a realistic course of action? And at what point do we know whether the actors have actually changed their behavior?

Mr. CHERTOFF. So, let me take a crack at this. And as—I begin by saying IP theft is not, in my mind, an act of war, but it's obviously wrong. I think one thing we could consider doing is this: If we see stolen IP actually being used by an enterprise, we could then, I think, go after the enterprise legally for that, and exact a serious economic injury.

And frankly, I think one of the reasons the Chinese agreed, several years ago, that commercial espionage to help their enterprises was not appropriate was a recognition that the sauce for the goose could become sauce for the gander as well. And I am not naive, I don't believe they have totally stopped it, but I do think that using that kind of economic leverage can help.

Mrs. DAVIS. Uh huh.

General ALEXANDER. I think it's the greatest theft of—and transfer of wealth in history, from our Nation. It affects our future generations. So that IP theft we have got to stop. I think sanctions and tariffs and other things are one way.

More importantly, we need to fix our defense. Right now, we are so porous because, as a Nation, we are doing point defense on every

point, and they are looking at this as a large target and only find one "in" and they are in. And everybody's going to make a mistake. So we have got to come up with a more comprehensive collective solution.

Mrs. DAVIS. Is—go ahead.

Mr. JOHNSON. I agree that IP theft is a significant problem, and it encompasses national security as well. Theft of intellectual property by nation-states is a significant problem that this committee should be very concerned about.

Mrs. DAVIS. Could you speak a little bit more to who's in charge? Because we talk about—excuse me—we talk about the integration of effort, and yet it's difficult, who actually is in charge? And when it comes to private companies, who do they see as in charge? What is their perception of who's actually making the rules?

Mr. JOHNSON. We—we made an effort at this in the last administration, and there's always the temptation, with every new administration, to try to reinvent the wheel. But in general, the Department of Defense, NSA [National Security Agency], Cyber Command, should be responsible for defending the Nation against an attack and the security of our military systems.

Law enforcement is—should be responsible for the threat response. In other words, you report the crime to law enforcement, whether it's the FBI, the Secret Service, or HSI [Homeland Security Investigations], and the Department of Homeland Security should be responsible for asset response, the forensics, patching the vulnerabilities. And so, the way I used to describe it when I was in office, "Jim Comey is the cop and I am the fireman, and you call both of us when you have an attack."

Mrs. DAVIS. Yes, yes. But at the same time, I think there's—you are—we are talking about a common operating theater, and are there authorities that still are unclear? And, you know, just to what extent have we been a little slower to come to that, so that—so that there is a common sense, or a common knowledge, really, of——

Mr. JOHNSON. Well, despite what I just articulated, I think that there is still a lot of—a lack of public awareness about who is in charge. And it has to be a whole of government approach, but the lines of authority need to be reiterated and stressed over and over——

Mrs. DAVIS. Is there a cultural problem in doing that?

Mr. JOHNSON. In my experience, cultural problems stem from the leadership. If the leaders of the organizations know and trust and respect each other, then that filters down in the culture. But leaders turn over. I thought at DHS we had an excellent working relationship with the FBI in part because Jim and I were friends for over 25 years. And that filters down.

But with each political turnover, with each new administration——

Mrs. DAVIS. Right.

Mr. JOHNSON. The personalities change.

Mrs. DAVIS. What role does the executive play in that?

Mr. JOHNSON. I think that it's important for the executive to reinforce continuity and consistency in the protocols and how every-

one should work together, so that it eventually settles in to how we approach this issue.

Mrs. DAVIS. Yes. Thank you. Thank you, Mr. Chairman.

General ALEXANDER. Can I add to that one? Because I think it's important. The question that you are asking is who's in charge. You know, we had—when we were starting out in standing up Cyber Command, Secretary Gates had some great ideas about how you pull together all of government into a comprehensive solution.

And he thought of, how do I pull what we are doing in the Defense Department, Justice Department, and Homeland Security all together, so that we can act in peacetime—seamless from peacetime to crisis to a war? And I think that's the kind of solution that we need to look at as a country.

And right now, as you note, it's fragmented. And it was great working with Secretary Johnson, it was great with Secretary Chertoff, but the reality is there are personnel issues, resource issues, technology things.

And I agree, the FBI was great to work with for me. You know, it was—they were amazing, and whenever—we would assume they would have had the lead because of law enforcement, but if it was nation-state it would flip to us.

So I think you need to figure out—we need, as a government, to put that together somehow. Some have talked about a Secretary of Cyber. I am not sure I would go that far, but I would sure look at how you nest between Homeland Security and Defense Department common authorities and a common structure between those to get that going, and append to that FBI.

The CHAIRMAN. Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman. Mr. Johnson, you went to school in Atlanta, at Morehouse, I know, and as we discussed earlier, and the city of Atlanta on March 22nd was attacked with—as I understand it, the SamSam ransomware. The people asked for a $51,000 ransom, a fairly small amount, but my understanding is that that group has raised almost a million dollars from different attacks, and these attacks have been going on since 2015, with that type of ransomware.

Now the $51,000 is not a whole lot of money to a city like the city of Atlanta. The damage that was done and the cost to the city of Atlanta is going to be in the millions, in shutting down courts, the inability to pay fines online, the loss of time of employees. I don't know what it will total up to, but it will be millions of dollars that the ransomware costs.

My question gets into, since this has gone on since 2015, the SamSam ransomware, has there been a coordinated effort from the U.S. Government to find out where these attacks, these SamSam attacks are originating and how will we stop them? And if we do find out where they are originating from and who is doing it, how effective are our laws with regard to the prosecution of that crime if it is in the U.S. or if it is outside of the United States?

Mr. JOHNSON. A coordinated effort to—you know, I don't know that there is, within the FBI, for example, a ransomware bureau devoted to those who engage in this, and as I think you point out, those who engage in ransomware are open and notorious. It's becoming a bigger and bigger business.

I suspect that—and Mike could probably speak to this, too—I suspect that the existing laws in title 18 are sufficient to deal with this as a crime, but in my experience, most often ransomware stems from a simple act of phishing or spear phishing, where an employee who uses the system opens up an email or an attachment that they shouldn't, and the actor is in the system and they can steal things in the system.

And so a large part of the answer to the ransomware problem is simply raising the awareness of those who use systems about opening emails that you don't recognize and attachments you don't recognize.

But I suspect and believe that the existing laws are probably sufficient to deal with this once you can track down the bad actor.

Mr. SCOTT. So one of the questions that has been asked of Mark Zuckerberg is about the fiduciary duty to protect information. So banks, financial institutions, the government, the city of Atlanta would have a fiduciary duty to protect the information that they had in their computer systems.

What about the networks? Should the networks have a fiduciary duty to protect the information that they are housing?

Mr. JOHNSON. A fiduciary duty, if not a legal duty, to protect the information that they are the custodians of. A bank certainly has a fiduciary duty to protect the information with which it is entrusted, and the management of these banks have fiduciary duties to their shareholders as well.

And so I am sure that there are certain obligations that those who manage networks have to the customers that rely on them.

Mr. SCOTT. I am short on time. I guess that the challenge I see in this area—if someone goes to work for a Google or an Oracle or a technology company, they may make in a month, if they are good, what we pay people in a year. And it—it seems to me that some way, some how, the laws are going to have to incentivize those companies to do everything they can to stop these types of attacks. Not because we don't have capable people, but because there's so much of it going on out there that we need—we need their help in doing this.

And so sometimes they see it—would see it even before—even before we would see it. So I have an Ag [Agriculture] meeting at the top of the hour, but I appreciate all of you being here, and thank you for your service to the country.

The CHAIRMAN. Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman, and I want to thank our witnesses for your testimony today and for your service to the country. Over the many years that we have all worked on this issue of cybersecurity, I have had the pleasure of having you testify before me, whether it's on the House Armed Services Committee, or the House Intelligence Committee, or the House Homeland Security Committee, and I have always deeply appreciated your thoughtful answers and your contributions to better protecting the country in cyberspace.

So, you know, the one question that I still continue to get from—from people back home is, you know, why aren't we more effective at defending the country in cyberspace? Why are we still seeing these high-profile cyber intrusions or attacks, if you will? And I—

you know, obviously the answer is we are getting better at it, but it's a very hard thing to defend against.

And we have the NSA with Cyber Command that is trying to—basically defending the dot-mil network. The Department of Homeland Security is in charge of defending the dot-gov network, although they don't have the policy or budgetary authority to reach government to actually compel departments and agencies yet to do what needs to be done. That's why I have long advocated for the bill I put in, the Executive Cyberspace Authorities Act, to have someone with that kind of policy and budgetary authority.

But yet most of the damage can still be done in the dot-com world, particularly in critical infrastructure, and no one really is in charge there, and no one has the authority, and I don't know the American people, you know, would accept—and I don't think they would accept having NSA or Cyber Command sitting on the network internally to defend in the dot-com world.

So, what is the best way forward to in fact defend the country? And, General Alexander, you and I have talked about this—you know, right now—and you have often referred to it as, you know, "We are still playing clean-up on aisle 9."

I am interested further in your thoughts about the idea of deterrence in cyberspace. The new U.S. CYBERCOM Command vision talks about defending forward as far as possible before adversaries penetrate our defenses. And this sounds somewhat like the old adage of the best defense is a good offense.

And so do you agree with this posture? And if we see things in cyber that—whether it's a nation-state or criminal enterprise about to do something—is it best that NSA or U.S. Cyber Command inform private industry about—about the impending damage that could be inflicted and let them defend or fix the problem? Should NSA or U.S. Cyber Command take the action to stop it, or turn it off, as you say?

What is the best way forward to handle these challenges?

General ALEXANDER. So first, I think the—in setting the defensive infrastructure, the first thing we need to do—and DHS would have the lead on—set the standards of what industry has to do. Here's how you lock your doors, here's how you encrypt your stuff. And set standards, and Congress can set incentives for small, midsize, large companies to do that. Then if they are attacked by something that exceeds those standards, they should have some form of protection.

And part of that standard should include sharing information under law—CISA-level information, not personally identifiable, but threat intelligence, cyber intelligence information at network speed with the government so the government can do what you suggest.

And it falls then on the government—who's role is it? If it's criminal, it's going to go to FBI. If it's a nation-state, and an attack that's going to hurt our country, that's where you want Cyber Command and NSA to be actively involved. And if it's foreign coming in, you want NSA's intelligence to help inform law enforcement and the defense on how to defend that government.

So I think the key thing that you can help do here is help industry set standards, give them the incentive to do that, and the liability protection if they meet those. Because the lawsuits are way

out—way out of bounds, and companies that are being attacked by nation-states don't have the ability to defend. Sir.

Mr. JOHNSON. So in the Cyber Security Act of 2015, Congress established limits on criminal and civil liability for those who share cyber threat indicators with the Department of Homeland Security. So that's a good thing.

The problem we have is—and we set up, on my watch, automated information sharing with the private sector—and Keith is right, there's a lot that private sector can benefit from if we at the national level are able to share the threat streams that we see, but there's also a lot that the government can learn from the private sector. Things that are happening within the private sector that the government doesn't necessarily know about right away.

I have been disappointed that not more entities in the private sector are willing to share information——

Mr. LANGEVIN. I agree.

Mr. JOHNSON [continuing]. With the Department of Homeland Security because they are concerned that it will go public, it will be compromised in some way, and that's a—that's a real problem, that's a real dilemma. There are many, including people in Congress, who believe that there ought to be mandatory disclosure by Federal agencies in certain circumstances if we know about something.

And that, frankly, compromises DHS's ability to encourage the private sector to come to us and work with us.

Mr. LANGEVIN. Well, my time expired, but thank you all for your testimony here today, and your answers, and I yield back.

The CHAIRMAN. Ms. Stefanik.

Ms. STEFANIK. Thank you, Mr. Chairman. I have three questions, and I am hoping to get through all three, so I will start with you, General Alexander.

You helped build Cyber Command. What steps do we need to take in this year's NDAA process to mature Cyber Command? And then, look forward 5 years. What does Cyber Command need to look like 5 years from now?

General ALEXANDER. I think first the unified command is the right next step, getting to a unified command. I think the rules of engagement discussion that we have is the second thing that I would push at. The third is with government as a whole, including Cyber Command, how do we defend the country?

How do we, as a government, work together to defend this Nation? And bring it out and have a public discourse on how we are going to do that. Don't go into the tools and all that, but talk about why the information that's being shared is necessary to defend this country.

Ms. STEFANIK. Thank you for that. My second question has to do with emerging technologies. When we consider what the world of cyber looks like, quite soon I think of threats like AI [artificial intelligence] and quantum computing. What—how do these technologies play into the future of cyber warfare, and we need to be thinking about as policy makers? I will start with you, Mr. Chertoff.

Mr. CHERTOFF. Well, I think on—on AI, as with most technologies, there's an upside and a downside. There's no question

from a threat standpoint the ability of an adversary to automate the ability to test and try to break into a network, or even to use that for kinetic purposes, increases the threat.

But the good news is I think, particularly if you use behavioral analytics, AI can be a good way of defending the network in depth, which is what we need to do.

Quantum computing, I think it raises some issues about encryption. And encryption is a major security tool. There's a view, however, that quantum computing can eventually make it very easy to penetrate encryption. It may also be the case, though, that it may be a tool to actually enhance encryption.

So in both of these cases I think we have to watch carefully to make sure that, to the extent the threat is increasing, we are using these technologies to increase our resistance.

Ms. STEFANIK. General Alexander, I will go to you next, but I want to also add an additional question related—are we underinvesting in these spaces?

General ALEXANDER. No, I was going to hit just on that, Ms. Stefanik. I think first we have to lead globally in quantum computing and AI. The country that is the leader in those two technologies will be the future superpower. That needs to be us. And so we aren't investing enough, and this is a huge area.

And there are some great experts in government at classified levels in both, and I would encourage you to get with those.

I think in quantum computing what Secretary Chertoff said is exactly right, both good and bad. AI the same thing, and you have seen Elon Musk and Gates go at this, both pro and con. I think the good part of it, it will help us solve cancer and other things, and I think there's tremendous good. The bad parts, it means your decision cycle is going to be extremely fast in cyber and the attacks are going to grow, so we have to be ready.

Ms. STEFANIK. Mr. Johnson.

Mr. JOHNSON. I agree with what Keith just said. I think that we need to invest in cyber talent in the Federal workforce. All of our best talent in the DHS, the people that can actually explain this to me, get stolen into the private sector because they are able to pay multiples of what we pay in the Federal Government.

Congress has done some things to enhance our ability to hire cyber talent, but I think that's definitely a work in progress.

Ms. STEFANIK. Thank you. And my last question I will try to get through quickly, each of you have testified to the importance of improving interagency coordination and information sharing. I want to drill down into the specifics. What specific actions can we take from the HASC [House Armed Services Committee] perspective to improve this interagency collaboration and ensure that we are improving our readiness?

Mr. CHERTOFF. So one suggestion—and actually back in 2008, General Alexander and I talked about this—would actually be to create—to co-locate representatives of the three major government agencies in a setting that would allow them to have a common operating picture in real time about what is going on.

General ALEXANDER. We actually built an integrated cyber center up at Fort Meade, where you would see the center of some of that, and so I would encourage that, to build that common operating pic-

ture so that you can see the attacks, and each part of government could coordinate what their response would be. Right.

Mr. JOHNSON. DHS has actually built an integrated cyber center, too, called the NCCIC, the National Cyber Communications Integration Center. And it's an interagency operation, and I think we need to bolster that and improve upon that.

Ms. STEFANIK. Thank you, my time is about to expire. I appreciate the answers.

The CHAIRMAN. Mr. Larsen.

Mr. LARSEN. Thank you, Mr. Chairman. I would like to yield my time to Mr. Khanna.

Mr. KHANNA. Thank you, Mr. Larsen. Thank you, Mr. Chairman. Thank you to our witnesses for your service to our country.

Secretary Johnson, I was very impressed by footnote 5 in your testimony, where you talk about the definition of cyber warfare. And you explain your view that we should have a limited definition of cyber warfare. One could imagine the Russians creating cyber dislocation in Latvia, and the last thing we would want is to be bound, under NATO, to go to war over that.

And I was surprised reading it that you wrote that we don't have a definition of cyber warfare in the government, and I would be curious about your thoughts of what Congress or the government should do so we have a clearly defined standard for cyber warfare.

Mr. JOHNSON. You are correct. We spent, in the Department of Defense, as some members of this committee will know, literally decades writing a law of war manual that I think started in the 1970s. And it was finally published in 2013 or 2014. And it barely touches upon cyber, because cyber didn't exist when we began writing it.

And so beyond answering the question, may a cyberattack constitute an act of war? There is a lot more that needs to be filled in in the blanks. You know, what constitutes a cyberattack? What are the implications of that? What are the acceptable parameters for how we respond? What are the limits on the private sector in their responses?

But the basic legal question is one I was interested in, and I basically defer to those who have already written on this, which is what I said in my statement. That you have to look at the kinetic effects rather than the kinetic means. And I caution against reaching for something that's too creative and too expansive, because it would have implications globally. And so it's sort of like be careful what you ask for.

But I think there's a lot more work that needs to be done, limited simply to cyber—if you will, cyber warfare, what constitutes a cyberattack, and what their—what are the acceptable protocols. And there are aspects of the existing laws of armed conflict that we can borrow from. Necessity, proportionality, distinction in a cyber response; I think there are elements of law of war principles that are useful in developing this, but it's something we have to undertake to do.

Mr. KHANNA. Well, I appreciate it. I certainly learned a lot, and I hope you will use your expertise to help guide this committee, Congress, and the Executive Branch as we try to define that, so

that we don't find ourselves in a war, escalating because of too creative or expansive a definition.

I was also struck, where you talked about the coordination in the private sector with cybersecurity. I mean, it's always struck me that we don't have companies having their own armies. That thought would be absurd. And yet, we have all of these companies having their own cybersecurity operations.

And the question, to any of the witnesses, is what can we do to make that less of a burden, so that if you are a small business or you are a company, you don't have to have your own army to protect your cybersecurity? Is there a role for the Federal Government to do this, like we have an Army, and an Air Force, and a Navy to protect our Nation?

Mr. JOHNSON. Well, it's the basic response of the national government to defend the Nation against an attack. And on the civilian side, law enforcement, the Department of Homeland Security can share information, encourage best practices, but at the end of the day, whether you are the CEO [chief executive officer] of a large public company or you are the manager of your own business, you have to be responsible for the security of your own systems. And there are a lot of outside experts that can help with that in the private sector.

This inevitably has to be a public-private endeavor, because of the nature of cybersecurity.

Mr. CHERTOFF. Yes, I would add to that, that I think for the smaller enterprises, there are now managed security services that can actually do that as an outsourced function. And one of the benefits they have is if they are working with a lot of different companies, they are seeing a lot of activity over the landscape, and that actually makes them better.

General ALEXANDER. And I agree with that approach. I think the key is, and this is where Congress could help, if you set standards through DHS that industry meets, and you are protecting against what I will call a reasonable threshold of attacks, and then somebody comes in with a nation-state-like attack, just as in the physical world, you have all your bank guards, you have all these folks working it, and if the—a motorized rifle regiment comes in and wipes them out, you would say, well, shoot, you should have had air defense systems.

And the reality is when it gets to nation-state level, you have to have nation-state response. I think getting there means everybody gets to a certain standard, and then shares at network speed across government so the government agencies can do their specified roles.

Mr. KHANNA. That's very thoughtful. I really appreciate the testimony of the witnesses on this issue.

The CHAIRMAN. Mr. Banks.

Mr. BANKS. Thank you, Mr. Chairman. Gentlemen, in my State we have already seen the consequences of cyberattacks. This past January, a criminal hacking group was paid $55,000 in Bitcoin as ransom to regain access to a hospital computer system at Hancock Regional Hospital in Greenfield, Indiana. This came at a time during flu season, when the systems and the information they contain was critical to providing health care.

With—while this was a criminal action by one group targeting a single hospital, the effects of a state actor using cyberattacks on the public health system or other critical infrastructure would be disastrous, given the systematic vulnerabilities.

So my first question, for all three of you, is since much of the Nation's critical infrastructure is privately owned, what if—what efforts need to be taken now to better secure cyberspace activities essential to their daily operations? And we can start with you, Mr. Chertoff.

Mr. CHERTOFF. Well, you know, I think this is—again, there's not a magic bullet answer to this. And the analogy I often use is the public health analogy. You know, how do we protect ourselves against disease and illness? It requires some things the government does in terms of formulating vaccines, but it requires us to take certain steps.

So in the case you are talking about, look, a lot of these ransomware attacks occur because somebody downloads something they shouldn't, or because you haven't patched or updated. And those are things which are on the responsibility of the private sector actor to do.

Then there are other elements, you know, particularly when you are dealing with a nation-state, where our ability to perceive that something is being readied for an attack could arguably call for us to act preemptively. Certainly, if there was the possible consequence of loss of life.

So I think this is—there's not going to be a single step, it's about raising the level of cyber hygiene for the owners or operators of the critical infrastructure. It's about backup for the critical data. It's about training people about the silly things they ought not to be doing. And then when you do see a nation-state fixing to do something, then there's a—I think room to have a discussion about do we act to blunt that away before it hits us at home?

Mr. BANKS. General.

General ALEXANDER. So I agree. I think setting the standards, getting everybody to build and work at those standards, and then sharing information across the government is the way to do this. Ransomware, the year of ransomware, of 2016, 2017, it's going to continue. They are making money on it.

And so the issue for the government will be how do we respond, between law enforcement, intel, and defense? And then what can we do in hygiene to help defend against that?

And I think that's where the common operating pictures of what you are doing for incident response and helping critical infrastructure, and what you are doing to defend the Nation need to be merged.

Mr. JOHNSON. I agree with everything that's been said. I would add to that that there are lots of people who are part of critical infrastructure who don't know that they are part of critical infrastructure. For example, arguably election infrastructure, before I made it explicit, was already part of critical infrastructure, because it's part of government infrastructure.

And so a beginning point is to educate those in critical infrastructure that they have a heightened duty, and, therefore, need a heightened awareness.

Mr. BANKS. So along those same lines, one of the difficult issues, culturally, for hospitals and other private sector entities is information sharing with the government about their systematic vulnerabilities. What—what can we or should we do to improve the culture of information sharing between the private sector and the government that would involve critical infrastructure? And, Mr. Johnson, we can start with you.

Mr. JOHNSON. We have already done a fair amount. Congress has already done a fair amount, as I mentioned earlier, by enacting limits on criminal and civil liability for those who share cyber threat indicators. DHS has established automated information sharing that has a privacy scrub that goes with it.

And I think it's really a matter of raising the levels of trust and lowering the barriers of suspicion that exist right now. And there's a lot more work that needs to be done there, because not enough in the private sector, in critical infrastructure, have the type of partnership that I think they need to have with DHS to effectively deal with this issue.

General ALEXANDER. I think for most hospitals—there's two hundred and some in New York City alone, they should outsource it and get a comprehensive solution across all of them. Their focus is on saving people. And if they are spending a lot of time trying to defend their networks and keep their equipment up, then they are not doing this. I think we have to look at it more like that. Secretary Chertoff brought up part of that, and I believe that's the correct way to go do it.

Mr. CHERTOFF. I would simply add to that, I think we need to educate hospitals and medical facilities that they are in fact critical infrastructure, and they are in fact targets. We have information sharing and analysis organizations that are platforms for sharing.

One other thing that I would say—and I have talked to people in the medical community on this—as we multiply smart medical devices that are connected to the internet, we have to be very careful we are not creating serious vulnerabilities that would lead to a loss of life. So pacemakers or various kinds of injection pumps, if they were wirelessly connected can be very beneficial, but the devices could also be an attack vector and we need to look to the FDA [Food and Drug Administration] as well as the industry to focus on that.

Mr. BANKS. Thank you. My time is expired.

The CHAIRMAN. Mr. Veasey

Mr. VEASEY. Thank you, Mr. Chairman. General Alexander mentioned something earlier, but I think that anyone can answer this. And I wanted to know, do you think that we should be looking at bolstering the military and State Department when it comes to dealing with this issue?

And the reason why I mention that is because it seems to me that if attacks on small to midsize allies are occurring, that they may—that that also may be an issue of governance that they have within their countries by not being able to manage all of this. And just wanted to know if you had any thoughts on that.

General ALEXANDER. I do think alliances are going to be extremely important in cyber. And it's important for two reasons. One, to get the norms and the group together, and second, we learn

a lot by seeing where others are attacking. Most attacks that hit our country are tested elsewhere. The more partners we have, the smarter we will be in defending ourselves.

Mr. VEASEY. And also, General Alexander, I wanted to ask you, because small and midsize allies in certain countries that we are trying to give assistance to, they have had trouble managing their natural resources. How—how do you help countries like that manage something as sophisticated as cyber, you know, defense? Like, how do you empower them to do that when they have had trouble just managing just basic needs of running a country, you know, previous to all the cyber issues that we had?

General ALEXANDER. So that's more difficult. I think there are some countries that you can help right off the bat, and I encourage our government to work with those that they can help protect. You can see a live fire, in terms of cyber going on in the Middle East. Partnering with the Middle East to help solve that is going to be extremely important. The same in Asia; we are seeing a lot of attacks. And in Eastern Europe.

Each of those have different groups. I was in a discussion with some of the folks from NATO a couple days ago. Doing a common defense with NATO and helping them set a standard would lighten our load, increase what they could do, and bring that collective body together as well.

Mr. VEASEY. And Secretary Johnson, I wanted to ask you, you said in your comments earlier that you think that there should—if you had your way, that you would have, in businesses and governmental entities, have some sort of minimal standards when it comes to protecting their cyber.

I wanted to ask you about the cost to that. Do you think that, in order for smaller or midsized businesses, and even smaller municipalities, to be able to really put the protections in place that they need—like, how much money would something like that run a smaller entity?

That could certainly be maybe a softer target, it wouldn't be as large of a target as a large city, but could certainly be a softer target. Like, what sort of resources would they need to bring to the table in order to meet those minimal standards?

Mr. JOHNSON. Well it depends on the nature of a business and the nature of the information it possesses and how it conducts business. Without a doubt, encouraging companies, either legislatively or otherwise, to embrace best practices probably means embracing a certain level of technology.

But we are all as strong as our weakest link. And so if you have a company in a supply chain that invest millions and millions of dollars in their own cybersecurity, but they do business with a supplier that doesn't, then the big supplier up the chain is at risk because they are doing business with somebody who doesn't see this as an issue.

But in my engagements in the private sector, I would encourage CEOs to view cybersecurity in the same way they would view physical security, the care and custody of their customers' intellectual property, and so forth, so that we don't view this as simply a side issue that's going to require some money.

It's a basic issue of security. As someone mentioned earlier, in many cases it implicates a fiduciary duty that someone may have. And so, sure, is it going to be an investment? Absolutely. But if you want to be the best at something, you have got to make investments in technology.

Mr. VEASEY. Right. And it would be interesting—my time is about to expire, and I will just add this at the end—you know, it would be interesting to get your comments on, like, as a—say a company that supplies a defense contract or a small, you know, midsize company that is a supplier—for them to be able to meet those same requirements could be much more onerous than the defense contractor, for instance. So, just something to think about.

Mr. Chairman, I yield back my time. Thank you.

The CHAIRMAN. Mr. Hice.

Mr. HICE. Thank you, Mr. Chairman. General Alexander, you are—you have made a recommendation to bring the responsibility for private sector outreach and the defense community under a single authority. Can you elaborate further on that, and why that's important?

General ALEXANDER. Well, I think having unity of effort is very important. And right now, everybody's really busy. And I look at how hard Homeland Security, with all the things that they are doing, Defense Department with what they are doing—when I was asked earlier by one of the members why aren't we making more progress, and the answer is everybody's busy handling a lot of things. Do you appoint somebody and hold them accountable for moving this, and going back to Homeland Security, and the Defense Department, and Justice to get it done?

I think the answer is yes. And where and how you place that entity is where I would get the Secretaries of Defense, Homeland Security, and Department of Justice together and say, iron it out. I think with Secretary Gates, Secretary Chertoff, in their seats back then, another couple of years and I think that would have been solved. And now I think what we need to do is look at that and say, how do you do that?

Because there are specific missions. You don't want the Defense Department going out and trying to police up all the incident response. You don't want them setting standards and looking—that's Homeland Security, and they have that, and they should do that. You want the Defense Department to defend the country. But both of those require for you to see this, and have this entire spectrum of cybersecurity visible to all the actors. It's not there. And we need to fix that.

Mr. HICE. I would like to hear the opinion from the other gentlemen. Mr. Chertoff.

Mr. CHERTOFF. I mean, I agree with General Alexander. I do think that there are distinct roles and responsibilities. The key is to have clarity about who supports and who's being supported in each of those roles.

Mr. HICE. Okay.

Mr. JOHNSON. I agree with that, yes, sir.

Mr. HICE. So all three of you agree that there ought to be a single authority, however that's decided, then? Now, when I walked in a little while ago, Secretary Johnson, you were touching on this,

so I would like to—I will just go to General Alexander—regarding how to improve the ability to recruit and retain our cyber experts. Do you have any thoughts on that?

General ALEXANDER. Yes. What we did, Congressman, at Cyber Command—we are not going to keep all these guys for a long time, but if you can get them to commit for 6 years, and get them in training for a year, this would be great for our country both in the military, in government, and then in industry.

So I think what the government can do is help train and educate a large population, not just for the Defense Department, but also for Homeland Security. And part of that training could be we will provide your training, you commit to a period of time in government.

And, you know, I really believe that young people should serve in government. I really do. And so this is a way to incentivize it, and you give them a future, and you help our country. That's what I would do. There are many young folks out there that can't afford college, but they are built for cyber. And we ought to latch on to them.

Mr. HICE. So what timeframe do you think they ought to be able to make a commitment?

General ALEXANDER. Well, I would go for 6 years, with one of those or one and a half being a commitment for education, and I would advance the education, similar to what the Defense Department does for the joint cyber ops [operations] center—school, but I would do that a little bit longer with some of the defense and all that, and I would mix them all together.

And the reason is you want the people that work in government to work together.

Mr. HICE. Okay.

General ALEXANDER. And so the military and civilian.

Mr. HICE. I see some head-nodding.

Mr. JOHNSON. I would concur with what he said. My message, when I was in office, to young people continually was if you want to—if you want to go work for The City Group, or Goldman Sachs, or J.P. Morgan Chase in cyber, come serve your country for a few years and get that benefit of those insights.

And then the struggle becomes they all are drawn to the, you know, perceived "cool" agencies, like NSA, and so we have to encourage them to want to work in the civilian agencies as well.

Mr. HICE. Okay. Last question. Is the—in your opinion, is the Cyber Mission Force adequately sized for the challenges it faces? General.

General ALEXANDER. I think it is right now.

Mr. HICE. Okay.

General ALEXANDER. What I would encourage is a set of exercises with that force with the rest of government, and perhaps key players from industry and Congress, to look at that and see the challenges. I think the teams and the construct of the teams were right. We have based those on other teams that were very successful for our country. So I think it was the right thing.

We were encouraged initially to cut it back. And I said, but this is what it takes. And we—40 teams of a certain type offensive, 68

defensive teams that would work with—DHS and others, and the 25 analytic teams. I still think that's right.

Mr. HICE. Thank you. Thank you, Mr. Chairman, I yield.

The CHAIRMAN. Mr. Garamendi.

Mr. GARAMENDI. First of all, Mr. Chairman, thank you for setting up this hearing. It's extremely important and the three gentlemen that are testifying have a wealth of wisdom.

If I might, recently the Department of Homeland Security issued a—an alert that Russia had hacked into critical civilian infrastructure, gaining access to our power grids, power plants, and other industrial plants, and in some instances, gaining operational control.

Is this an act of war? I think that word was used by the Department of Homeland Security. If yes, what is the appropriate response?

Mr. JOHNSON. Congressman, I would characterize what is in that statement as a very significant threat to our Nation and our national security, but I would not characterize it, in and of itself, as an act of war.

Mr. CHERTOFF. I agree with that. I mean I think that—and it's often difficult to tell when you find malware in a network, what the purpose of it is. And often it has multiple purposes.

You know the—it could be at one level, reconnaissance. It could be deterrence in the sense of a way of signaling to the U.S., look what we can do and, therefore, if you mess with us we are going to do this. Or it could be prepositioning something for an attack, or all three of those.

But I would agree with Secretary Johnson that positioning is not the same thing as actually carrying out an act of war. Now, if you shut the lights off and there was a serious loss of life, then we are getting into territory——

Mr. GARAMENDI. Well, they did shut down a reservoir, if I recall correctly.

Let me just move on. So, it's not an act of war. That brings us to the rules of engagement, doesn't it, and to the definition thereof. We are not going to get to that today, but both of you—all of you have said this is critically important.

General Alexander, you have danced around this issue of being able to comprehend when an attack is underway, and to be able to act. You haven't been specific about that. If you would take a moment or two to discuss that, and then my final question is, we have an annual exercise with CYBERCOM working with DHS and so forth.

Let me just—I am going to hold General Alexander my question. Do you all want to stay with this other question I had.

So that annual exercise would seem to be exactly what this Russian intervention—we won't call it an act of war, but intervention into our critical grids, was designed to deal with.

So what comes of this? Should we not be using the techniques that come from that annual exercise to deal with this Russian hacking into these grids?

General ALEXANDER. Sir, I think the issue for them hacking into this grid is they are trying to gain insights into the operations of our network for future use. I agree with what Secretary Chertoff

said. I don't think this is an act of war. I think it's an act of intelligence gathering and positioning for future conflict.

What it does show you is that we have to have visibility of those types of attacks. So you asked specifically, what does that mean? And I will give you an example.

If you look at what happened to Saudi Aramco, the destructive attack into Saudi Aramco with a wiper virus actually went on for about 2 months. No one had insights into that because nobody's looking at Saudi Aramco. And our government cannot see today actively what is going against our energy sector.

The energy sector actually has been the great—the best to work with in this area. They are pushing to really step that up. I think their—their strategic infrastructure, coordinating council and things that they put forward is exactly right. But it needs to go to the next step. How do you get that data up to government so you can build that picture so you can see Russia coming in.

And the answer is you don't see that. NSA doesn't see it, CYBERCOM doesn't see it, DHS doesn't see it. So what happens is they are getting hit, they are—they don't have the ability to share it. They don't know they are getting hit or they would have stopped it. So our common operating picture, it's like it's free for them to get in. We have to build the system up and make that visible.

Mr. GARAMENDI. We are going to write the National Defense Authorization Act in the next 2 months. What should be written into that to deal with this precise problem?

Mr. ALEXANDER. Well, I think it's to build a common operating picture and sharing. I would emphasize that the CISA Act of 2015 and take it to the next step and say—and encourage companies and government to work together and to train and practice so that—I would look at this as strategic infrastructure coordinating council and encourage councils like that, where you bring industry into government to share this information is exactly right.

That puts CEOs in the seat.

Mr. GARAMENDI. You used the word encourage.

General ALEXANDER. Strongly. I don't know what you can do with industry, but you know——

Mr. GARAMENDI. Encourage them hard.

General ALEXANDER. I think—I don't know that you need to mandate it, because I do believe they are sitting forward. They want help. They want the government to help them. They know they can't defend against a nation-state. And they know that—especially in the energy sector, they are critical to the future of this country.

Mr. GARAMENDI. I am well over my time. I will yield back, but I would love to have you gentlemen help us write that encouragement.

The CHAIRMAN. Ms. Hartzler.

Mrs. HARTZLER. Thank you, gentlemen. I appreciate your expertise and insights on this really critical issue. The Missouri National Guard was the first State to fully staff a National Guard computer network defense team to respond to cyber threats and attacks. And this unit, located at Jefferson Barracks in St. Louis, is consistently sought out to train both National Guard forces across the country as well as Active Duty.

These National Guard members are in a unique position because they can utilize their civilian roles, training, and expertise into their military cybersecurity roles. And I think we can all agree that the private sector moves faster with technological innovation so by using citizen soldiers, we can leverage new ways of thinking into the military. So what do you think should be the force structure of Active Duty, Reserve, and National Guard cyber warriors? I am not sure who wants to start off.

General ALEXANDER. So actually, you have hit on it. When—at Cyber Command, we encouraged, and we had several States set up National Guard with cyber forces—Delaware, Mississippi, Washington, and others for just that reason. I think that is an exceptional way and you hit all the key points. There are great people in the commercial sector who want to help the government but they don't want to sacrifice the—the pay.

So they can do both and they do—and there are great people there. I think that's exactly the way to go. The issue that will come up is now how do we bring those all together for the common defense, as things go from peacetime to crisis to war, something that we need to look at.

Mrs. HARTZLER. And I think you mentioned as well that they are—you support training them and then having a 6-year requirement. In a way, this kind of fulfills that a little bit. We train you and then you can go out in the private sector, but then come in on the weekends and you bring your expertise and to address things and be called up when needed. Secretary Chertoff.

Mr. CHERTOFF. Yes. I was going to say, I think that it is a little bit like the ROTC [Reserve Officer Training Corps]. I think that's a great idea. I mean, these days, we are looking to train people for the 21st century skills. If you bring them in and you train and they make a commitment to serve Active for a period of time and then they work in the National Guard, that's a win-win for everybody.

There are two other advantages. One is the relationships that are built wind up, you know, going on beyond the actual term of service. And one of the things I learned in law enforcement was a lot of the sharing and a lot of the coordination comes from personal relationships. And secondly, in terms of a common language and a common approach, it gives you a baseline commonality.

So I mean, I—if you were going to do something relatively dramatic, I think having an ROTC-type program to train and get service in this area would actually be a real benefit.

Mrs. HARTZLER. Makes sense. When I visited this unit, even though it's not in my district, I was so impressed. Several of them said we are in charge of security for Fortune 500 companies. And we see things during the week. And we are saying oh my goodness, we need to come—when we come back on—on our Active Duty assignment and apply those things to protect our Nation. So it makes sense to me. Mr. Johnson, did you—were you wanting to add something there?

Mr. JOHNSON. No, I endorse everything that's been said.

Mrs. HARTZLER. Oh, good. I wanted to go back, General Alexander, to something you said that piqued my attention in your testimony. And then just recently, as you were talking about integration of infrastructure. And I understand this isn't quite the same.

But there's a lot of discussion about the DOD's contract and building the cloud and whether it should be one cloud or whether there should be multiple clouds that we would use. Do you have an opinion on that?

General ALEXANDER. Well, I think in any instance, a cloud provider is going to have multiple instances. And so I would look for multiple instances for resilience. And no matter which one you choose and how you choose it, that means you don't put all your eggs in one facility. So when you think about the cloud, they build up a huge set of capabilities in a facility and then they build multiple facilities to give you that resilience.

I would look at the facilities, the resilience. And there are tremendous companies out there doing cloud capabilities and that's growing. I think that's part of the future, especially for mobile communication.

Mrs. HARTZLER. Okay. And the last question. Switching gears a little bit. What are we doing to mitigate the exfiltration of massive amounts of unclassified data from our cleared defense contractors? And is it working? And what would you do differently to protect this data? Who's going to take that?

General ALEXANDER. Well, I worked with the defense industrial base [DIB]. And great people. I would pull them together into an integrated infrastructure, call it a DIB infrastructure that works together so you can see what nations are going after defense information or related information, encourage those. We actually ran that. When you were the general counsel, we would call the defense industrial base working group.

We didn't go into it to that level, but I would build that up analogous to the way we recommended doing the same thing for small and midsize agencies, I would do that and offer that the DIB as part of the way of them bringing in. So beyond FedRAMP [Federal Risk and Authorization Management Program], which is the standards that they have to achieve in cybersecurity, I would go for a collective security approach.

Mrs. HARTZLER. Thank you. Yield back.

The CHAIRMAN. Mr. Gallego.

Mr. GALLEGO. Thank you, Mr. Chair. Kind of attaching some questions onto my good friend from Missouri, you know, and talking to some of my friends, we have to—we have a dearth of actual capable cyber warriors. And I had some friends that I served with in the war that actually came out and created and went through all these different programs to actually retrain them to being quote, unquote "cyber warriors." I have heard criticisms from colleges and universities that these programs are too staid and too static to adequately train students for the real world threats that are always changing.

So do you, one, see the quality and quantity of cybersecurity graduates as a problem? Number two, if so, what can be done to improve the dynamism and efficacy of cybersecurity education currently right now through our public and private schools or any other methods. We need to start from left to right.

Mr. JOHNSON. Well, I have to say I have been impressed recently when I've visited colleges and universities at the level of interest in a cybersecurity education. And very often there's also an interest

in serving in national security in cybersecurity. It doesn't surprise me that you you have heard some of the concerns that have been expressed because really of the newness of the topic.

And so there probably needs to be a concerted effort at who are the educators because this is rather new generation phenomenon, so a lot of interesting stuff——

Mr. GALLEGO. And who is going to be providing the curriculum also. I know the educators are important, but also sometimes the educators are behind the eight ball when it comes to curriculum.

Mr. JOHNSON. Correct. Right. I agree with that.

General ALEXANDER. So let me just add. DHS and NSA actually have a joint venture to work with colleges to set up a level of curriculum. So I think that's a great starting point. More importantly, look at the change in technology. It's doubling every 2 years. That means half of what kids learn in their freshman year is outdated by their junior year.

So we are training people for technology that doesn't exist, hence the problem that you bring up. Using applications that haven't been created. And so what that means is we now need to teach people how to learn, not just what to learn. And that's got to be part of this whole process and that's what I think you are actually getting to.

Mr. CHERTOFF. I would agree to that. I think a critical point is what you are doing is training people how to train themselves and that way can be a continuous process because it's not going to be like most subjects where you learn it and then it remains current. It's going to change very very quickly.

Mr. GALLEGO. In many of the universities that I visited or even community colleges there is usually like a corporate advisory board just basically that meets with the professors and with the educators who create a curriculum that is always staying up to date with whatever changes. Not to just obviously, cybersecurity or technology, but whatever field that they are working on.

What is our equivalent in our government to that? Is there a working group of both national leaders, defense leaders, as well as private sector leaders that are helping—who are helping our educators, whether it's community colleges or universities, keep up to date the curriculum? I know we kind of hit on that, but is there an actual formalized structure for this kind of interaction?

General ALEXANDER. So they actually do that between DHS and NSA, and now Cyber Command. They update that curriculum all the time and it's on the web so you can actually go to the information assurance director dot-gov I think is the IAD [Information Assurance Directorate]. And I think DHS has the same one. And it lays out all the standards and they update that continuously.

Mr. GALLEGO. And then is the private sector at all involved in this curriculum—making of this curriculum?

General ALEXANDER. Well to the extent that they reach out, but they aren't part of the accreditation process.

Mr. GALLEGO. Right

General ALEXANDER. I believe they provide input from both DHS and NSA.

Mr. GALLEGO. Understood. Thank you. I yield back.

The CHAIRMAN. Mr. Bacon.

Mr. BACON. Thank you, Mr. Chairman and I want to thank all three for your service and your leadership. Appreciate you being here. I have a few questions for General Alexander, and if time permits, one for the whole panel.

First of all, for General Alexander, right now we have one four-star for NSA, Cyber Command, and the two deputies, the three-stars, sort of run those organizations. But that provides us cohesion, unity of command, but yet I know there's proposals to provide two different four-stars, one for each NSA and Cyber Command.

And I fear that that will pull those teams apart, because I know and you know—I am a cyber and SIGINT [signals intelligence] guy by trade as well—that our intelligence seems to be closely linked with our offensive and defensive capabilities. I would like to know, where do you fall on this, and where are we at with this discussion?

General ALEXANDER. Well, I—I actually believe you have to have unity of command. If the decision is made that it's too big for one person, and then you put two four-stars, you then have to put somebody over top of both of them.

Mr. BACON. Absolutely.

General ALEXANDER. Between them and the Secretary [of Defense] and the DNI, and so that creates additional infrastructure.

So before we do that, I would encourage us to look at how we are going to fight in cyberspace, and the roles and missions of both NSA for reconnaissance and Cyber Command for military actions. And NSA may have responsibility in covert actions——

Mr. BACON. Yes.

General ALEXANDER. So you have this nesting. I think I would look towards unifying versus diversifying those capabilities.

Mr. BACON. My experience is the same. I just know there's proposals here to do that, to separate it, and I think it would be damaging to the cyber mission, because the intelligence portions of this are so closely linked to our offensive and defensive, you can't have two four-stars with two different priorities and keep those teams cohesive. So I just wanted to make that point, and I appreciate that you feel the same way.

On the cyber mission teams, are we fully operational, or initial operational? Where are we at?

General ALEXANDER. Well, so I am a bit dated. I have talked to Admiral Rogers, and they have made great progress. My understanding is they are, in most of them, fully operational-capable, but I am not sure how many of the 40 are at the level and where they have tested them.

So I know we were making progress 4 years ago. I have not kept up specifically on that. I do think this will get back to—now we have another group that we are going to be training, and always going through, so I don't know the answer to that.

Mr. BACON. Okay, thank you. One more question, and then I have got one for the panel. I think you talked about the right to self defense? Let me just play on that a little bit. I think, if we are only defensive—if we play defensive only, it doesn't serve deterrence well, and I think it makes us more of a punching bag.

I think we do need to have some—to practice some of our offensive muscles, mainly to serve as deterrence and make attacks on

us less often. Are we doing enough in the offensive realm to show, hey, when you attack us, you are vulnerable for a counterstrike?

Where do you all—and I'll open it up for anybody, if you feel like we are in this—in the right spot here.

Mr. JOHNSON. Congressman, as long as our intelligence chiefs tell us that certain nation-states are continuing to engage in bad behavior against us in cyberspace, then we—then the answer is no, we are not doing enough, obviously.

And nation-states, whether they are communist regimes, dictatorships, monarchies, all behave a certain way. They all decline to engage in behavior that is cost-prohibitive if there is a sufficient deterrent in place.

And to go back to what you said earlier, I believe that components of an effective defense can also include offense.

Mr. BACON. All right. Yes, go ahead, sir.

Mr. CHERTOFF. Yes, I would, I would agree. I would say there are two elements in deterrence. Deterrence by denial, which means we raise the barrier to doing something, and deterrence by response. We have done some things, particularly lately, that are a little more responsive, but as we see bad behavior we may need to dial that up a little bit.

And the one thing I want to just be careful about is not to treat the issues about information operations as the same thing as cyberattacks——

Mr. BACON. Right.

Mr. CHERTOFF. Because that raises a whole set of complicated issues.

Mr. BACON. Intelligence versus offensive is——

Mr. CHERTOFF. Correct.

Mr. BACON. Totally two different things, and reconnaissance has a long history of being not a combat operation, so I totally agree. And it's my feeling, too, that we are not showing enough teeth or offensive muscle and it doesn't serve deterrence well. It makes us more vulnerable to the other nations' attacks. One last question. And this gets to some of the earlier questions on the energy grid.

I am deeply alarmed by it. I think we are vulnerable to the next December 7th not being airplanes and torpedoes, but rolling blackouts and—and havoc in our society. Are we doing enough to build resilience in the defensive realm to protect our energy grid? And I realize that is more of a homeland security perspective.

Mr. JOHNSON. I have been impressed that certainly larger entities and public utilities recognize their vulnerabilities and the risk and are doing a fair amount. Again, I come back to the importance of information sharing about threat streams. And no matter how sophisticated you are, you can always benefit from more information, the larger picture at work.

And that's where I think we need to continue to focus and where I think Congress should continue to encourage the private and public sectors to work together and share information.

Mr. GAETZ. Thank you, Mr. Secretary. I am out of time, so I yield back. Thank you.

The CHAIRMAN. Mr. Panetta.

Mr. PANETTA. Thank you, Mr. Chairman and thanks to the three gentlemen who are here today. I appreciate you being here as well

as, of course, your stellar service, so thank you very much. Clearly cyberattacks are one of the main tools of what has been termed lately as guerrilla geopolitics, and what are being used more and more by the revisionist powers that we are hearing about.

You today have done a good job saying what is not an act of war. And Mr. Chertoff, you started to get to the point in—in Mr. Garamendi's questioning about shutting off the lights, significant loss of life. Could the three of you please give me further examples—in your opinion, obviously, of what you would feel would qualify as an act of war using this tool?

Mr. JOHNSON. Congressman, any cyberattack that has kinetic effects—physical destruction, death, physical injury—in my judgment would constitute an act of war.

Mr. CHERTOFF. I agree with and I—what I would emphasize is this. It's effects based. It's not based on the particular tool. Whether you are dropping a bomb or you are—you are sending something over a network, if you are killing people, that's an act of war.

Mr. JOHNSON. For example, we look at chemical weapons and we measure the impact by the effects that chemical weapons have, then we see the images. So I think you have to focus on the effects.

Mr. PANETTA. Understood.

General ALEXANDER. I would add in intent. So there I believe you are going to see some countries who push out something—and we have seen this already here in our country, where the attack was going against a different—but the malware hit our country and hit some of our industry. The intent wasn't to hit us. It was the collateral damage, not an act of war, but something that they should be held accountable for. I do think so.

If they have the intent to do us harm and they have the kinetic effects to go with it, I believe that's an act of war.

Mr. PANETTA. And if the means were solely done through cyber, should the response be solely done through cyber?

Mr. JOHNSON. As a legal matter, the answer is not necessarily. There—there is no legal requirement for a response in kind.

General ALEXANDER. Yes. And I—I agree. I think you want to hold all the elements of power and give the administration the authority to use them all.

Mr. CHERTOFF. I also agree.

Mr. PANETTA. Good. Good. And are—I would imagine the three of you are familiar with the Tallinn Manual 2.0. Would you feel that this is—that basically that the principles that are articulated in this under international law, are they effective?

Mr. CHERTOFF. It depends what you mean by effective. I think that international law and law of armed conflict ought to apply against cyber as well as kinetic. Whether people are observing them is a different issue. Where the challenger becomes, it's easier to mask what you are doing in cyberspace, generally, than what you are doing in the physical space.

So you get a lot of denial and deniability, which is why ultimately, enforcing the rules comes back to the level of certainty you need to have with attribution. The value of this, though, is—particularly with respect to our allies—and I have had discussions with them about this. If they agree with us that there's a violation of international law by what another country does, then they are

prepared to take countermeasures that would be more vigorous than if they viewed it as not being a violation of law of armed conflict.

Mr. PANETTA. Would you agree? Great. And Mr. Johnson.

Mr. JOHNSON. The one legal issue that I think deserves a lot of attention in this area are the principles around neutrality. We talked about this earlier and Mike talked about this earlier, where there's a nation-state that is doing something directed at us, originating from a neutral country. And the current principles, frankly, are insufficient to deal with this problem.

And it's something that we confronted time and again at DOD, and I am acquainted with at DHS. And so I think that more thinking needs to be put into what do you deal with when an attack is originating from or working its way through a neutral country. How do you deal with that?

Mr. PANETTA. Got it. Got it. Gentlemen, thank you. I yield back. Mr. Chairman, thank you.

Ms. STEFANIK. Mr. Carbajal.

Mr. CARBAJAL. Thank you, Madam Chair. Enemies that wish to destabilize our democracy have found a new frontier that I believe we are not adequately prepared for. And as you have touched on in your testimony. Today, I am interested in the role of the National Guard in response to a potential cyberattack. As a military asset with dual State and Federal roles, I believe they have a critical role to play in protecting our Nation's critical infrastructure.

If a cyberattack were to shut down critical infrastructure sectors such as the electrical grid, water, banking or transportation systems in California, an interagency response would be necessary. Law enforcement, first responders, owners of infrastructure sectors, the National Guard, and other Federal and State entities must have an integrated response and know how to work together. This requires us to train in a more integrated environment.

In this regard, I believe there is a significant training gap. Currently, there are no local programs in place that I am aware of for cyber network defense teams to receive continuous training to defend the Department of Defense information networks while exercising their defense capabilities in a State environment. Army cyber protection teams currently report to Fort Meade to receiving training in their title 10 mission.

But they still lack training relative to defending critical infrastructure. In California, the National Guard has embarked on a collaborative multiagency cybersecurity training effort that provides an environment specifically created for integrated training, allowing them to exercise their defense capabilities in both a Federal and State environment. Now, I know you have touched on this already, but I am hoping that you could elaborate on it a little bit more.

What are your thoughts on the need to expand integrated training efforts, including interagency cyber training facilities?

General ALEXANDER. So I think we absolutely need to do it. And you bring out some good points in terms of what are the roles and responsibilities at the State level, what are the roles and responsibility at the Federal level, and how do you connect those two? And

then how do you build both the bridges to the private sector? And all of that has to work seamlessly together.

I think it's about training. I think, first and foremost, we have to come up with a vision of how we are going to defend this country in cyberspace and get everybody to agree. That's part of that common operating picture.

With that picture, then, the second question that you just posed is, so, what is the role of State and National Guard and other forces in helping to accomplish that mission? How far can they go? Because what you don't want is States that independently attack back, you want them to defend. Or if they are going to attack, to be part of the Federal—the national response, not individual.

So we have to ensure that all that is bound together. And that is a tremendous training requirement, from my perspective.

Mr. JOHNSON. I agree with everything General Alexander said.

Mr. CHERTOFF. I would add one thing. I would like the training to include not only defending, but the ability to recover when something goes down, as we do in the area of training the National Guard when we have a natural disaster.

Mr. CARBAJAL. Thank you. And a follow-up question. I know this has been touched on as well today. Cybersecurity is such of a—a complicated issue. And you touched on earlier about threats emanating from neutral areas, or neutral countries.

How—how difficult is it to pinpoint the origination of the attack? Is it 100 percent of the time, we ultimately get to that source? Or sometimes we never get to that source? What is the percentage success rate, that we are aware, in pinpointing the actual threats? Because that leads to attacking, or counterattacking, somebody who may or may not be the original source.

Mr. JOHNSON. In my observation, it's often the case that we can identify where the attack is originating from, what platform, but then the challenge becomes: Who's pulling the strings? Who's ultimately responsible, and who's ultimately orchestrating the attack? And I am sure the other two witnesses will have views on that as well.

General ALEXANDER. I actually agree, and Secretary Chertoff brought some of those same points out earlier, that you can see where it starts from, so it might start in Russia, but Russia could say—Russian government could say, "That's not us, that's a hacker, he is outside."

Having said that, the problem that our companies would have in the National Guard and others is they can see the last point coming to them. What they can't do is see all the other points leading back to Russia. That's where your national intelligence system has to work, and it goes back to Mr. Bacon's question. You need to have the ability to see that whole threat and then respond, title 10 and title 50, integrated.

And so I think that's going to be the key for our country.

Mr. CARBAJAL. Thank you very much. I yield back, Mr. Chair.

Ms. STEFANIK. Thank you. That concludes our member questions. I want to thank the three witnesses here today for sharing your policy expertise and your recommendations as we move forward.

Just as an announcement, the Emerging Threats and Capabilities Subcommittee, which I chair, is having our cyber posture hear-

ing at 3:30 p.m. with Admiral Rogers and Assistant Secretary Ken Rapuano to continue this conversation.

Thank you very much for your service to our Nation, and this hearing is adjourned.

[Whereupon, at 11:55 a.m., the subcommittee was adjourned.]

A P P E N D I X

APRIL 11, 2018

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

APRIL 11, 2018

Hearing before the
House Armed Services Committee
"Cyber Operations Today: Preparing for 21st Century Challenges in an Information-Enabled Society"
April 11th 2018

The Honorable Michael Chertoff
Former Secretary of Homeland Security 2005-2009
Co-Founder and Executive Chairman, The Chertoff Group

Introduction

Chairman Thornberry, Ranking Member Washington, distinguished Members of the Committee, thank you for the invitation to discuss the current cybersecurity challenges and threats facing the homeland from Russia, China, and other nation-state actors and for providing me the opportunity to recommend ways to better prepare the government to face the challenges posed by advances in the cyber domain. I am pleased to join Secretary Jeh Johnson and General Keith Alexander who have both been prominent leaders on these issues.

The most recently-released 2018 Worldwide Threat Assessment published by the US Director of National Intelligence (DNI) warns that: "Competition among countries will increase in the coming year as major powers and regional aggressors exploit complex global trends while adjusting to new priorities in US foreign policy. The risk of interstate conflict, including among great powers, is higher than at any time since the end of the Cold War … Adversaries and malign actors will use all instruments of national power—including information and cyber means—to shape societies and markets, international rules and institutions, and international hot spots to their advantage."[1]

High-powered offensive tools are increasingly available to threat actors and have contributed to an uptick in cyber-attacks. Cyber-attacks are growing both in number and in sophistication and the scale of the theft of data has dramatically expanded in recent years. Broadly speaking, there are three categories of campaigns we see nation-states, to some degree or another, pushing. One is for intelligence purposes. The second issue is information operations designed to influence our institutions and societal norms. The third and most concerning dimension includes attacks that are designed to enable a military action or to threaten or carry out disruptive or destructive attacks.

Nation-states or state-sponsored actors will continue to use cyber means to gain advantage against the US from a political, financial, and military perspective. As noted in the World-Wide Threat Assessment, Russia will continue to attempt disruptive cyber operations with the intent to degrade democratic values as well as global alliances. Russia's wide range of operations include disruption of Ukrainian energy distribution networks, hack-and-leak influence operations, distributed denial-of-service attacks, and false flag operations. In the next year, Russian intelligence and security services will continue to probe US and allied critical infrastructures, as well as target the United States, NATO, and allies for insights into US policy. China will continue to view information warfare as military strategy and leverage cyber espionage to support its national security priorities. Cyber efforts from Russia, China, and other state-sponsored actors could have a detrimental impact on private companies, critical infrastructure, and our democratic institutions in the years to come.

[1] *See* https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

As I understand it, we have three Agencies responsible for defending against cyber-attacks: The Federal Bureau of Investigation (FBI) as the lead for law enforcement, the Department of Homeland Security (DHS) as the lead for critical infrastructure and defending government computer networks, and the Department of Defense (DOD) as the lead for defending the homeland, defending military computer networks, and developing and employing military cyber capabilities. There is no doubt that we have the capabilities necessary to counter and respond to the threats the US government faces from our adversaries. However, we must have a clearly defined strategy and develop policies to reflect that. In my testimony today, I will recommend ways for the US government to enhance our defenses through defining a cyber warfare doctrine that determines the level of attribution, simplifying information sharing programs between the public and private sectors, and incentivizing businesses to develop cybersecurity solutions to defend the homeland.

Understanding the current threat environment is essential if we are going to craft effective policy and defenses. I am therefore pleased to see the Committee's continued focus on this subject and appreciate the opportunity to provide my insights.

Data Theft for Intelligence Operations

A series of major thefts of personal data — not intellectual property — over recent years could suggest that a nation-state is trying to build a database of all Americans. This poses a threat to our national security because a nation-state could leverage this data for intelligence operations or influence campaigns.

- **OPM Hack:** The US Office of Personnel Management hack in 2014 was particularly worrisome. The White House said in 2015 that more than 21 million Social Security numbers, 1.1 million fingerprint records and 21.5 million forms with data like someone's mental-health history were stolen.[2] With technologies such as artificial intelligence, a hacker could generate useful information for intelligence operations from large sets of data. For example, a malicious actor could use the data to determine whether a corporate individual is really a government employee. The theft of fingerprints, as in the OPM attack, could also prevent government officials from going undercover in the future.

- **Yahoo Breach:** The recent Yahoo Breach is another example. Yahoo lost over 3 billion user accounts in two operations – one of which involved the engagement of two Russian Intelligence Officials[3]. The FSB, Russia's primary security service, allegedly hired the hackers to target US and Russian government officials, diplomats, military personnel, Russian journalists, financial sector employees and activists. The involvement of Russian spies suggests this was partly designed to aid espionage activities and is further evidence that the line between nation-states and criminal actors is becoming increasingly blurred.

Data Theft for Influence on Societal Norms

The Russians have weaponized the use of data to enhance and support their influence operations. In 2016, we saw an attack on the US Presidential election, an operation that the US Intelligence Community (IC) attributed to Russia. Russia also continued its influence operations in other countries of Europe. Ultimately, Putin's goal is to diminish the power and influence globally of the US and to shatter or splinter NATO.

- **Robert Mueller's Indictment:** A federal grand jury has indicted 13 Russian nationals and three Russian entities for alleged illegal interference in the 2016 presidential elections. The indictment says that a

---

[2] *See* https://www.opm.gov/cybersecurity/faqs/
[3] *See* http://fortune.com/2017/10/03/yahoo-breach-mail/

> Russian organization called the Internet Research Agency sought to wage "information warfare" against the United States and to "sow discord" in the American political system by using fictitious American personas and social media platforms and other Internet-based media. The indictment details an extremely sophisticated conspiracy in which defendants traveled to the United States to conduct research, employed specialists to fine-tune social media posts to "ensure they appeared authentic," and stole real people's identities to purchase online ads.

Russia will continue using propaganda, social media, false flag personas, and sympathetic spokesmen to build on its wide range of operations and exacerbate social and political issues in the US in 2018 and beyond. DHS and the IC must define a clear strategy to remedy this vulnerability. In his testimony in March, DNI Coats told Congress that the United States was "under attack" and yet there seems to be no strategy to combat this threat.[4]

Deterring a repeat of this conduct must be a priority for the entire US government, and indeed for all nations whose elections are susceptible to Russian interference. The need to impose costs is clear, but the challenge is to impose them in ways that matter to the Russian regime—not in ways that are projections of what would matter to the United States. Last week's imposition of sanctions on 7 Russian oligarchs and 12 companies under their control was a good start.[5] However, we cannot rely on deterrence alone: we need to ensure the United States has capabilities on the shelf to prevent and preempt this kind of behavior ahead of the 2018 midterms, and we must make ourselves harder to hack by improving our defenses and becoming more resilient.

- **Election Security**: One tactical issue that Congress must take responsibility for is securing our electoral data. Chicago's Board of Elections reported that names, addresses, dates of birth, and other sensitive information about the city's 1.8 million registered voters had been exposed on an Amazon cloud server for an unknown period of time.[6] Worse, it appears that hackers might have gained access to employees' personal accounts at Election Systems & Software, a major election technology vendor—information that could be used to hack a future US election. American elections are an increasingly easy target because our election technologies are antiquated and we have few federal level cybersecurity standards. An estimated 43 states rely on electronic voting or tabulation systems that are at least 10 years old. A survey of 274 election administrators in 28 states found most believed that their systems need upgrades. This is a matter of national security, and Congress should treat it as such. The $380 million in funding for election security that was included in the FY18 omnibus spending bill is a step in the right direction. The immediate funding will help states to replace outdated technology and improve cyber-defenses ahead of the 2018 and 2020 elections. A fair and safe election is one of the hallmarks of our democracy. While funding in the omnibus is an essential first step, it's just that – a first step. Congress should take up the full Secure Elections Act without delay, so we can fully protect the security and integrity of our elections.

Data Theft for Disruption

We have seen the rise of disruption attacks over recent months. This is the most concerning type of attack as they could be designed to enable a military action or to advance a geopolitical struggle and they could have devastating impacts on our critical infrastructure.

---

[4] *See* https://www.usatoday.com/story/news/politics/2018/02/13/intelligence-director-coats-says-u-s-under-attack-putin-targeting-2018-elections/332566002/

[5] *See* https://home.treasury.gov/news/press-releases/sm0338

[6] *See* https://www.wsj.com/articles/congress-can-help-prevent-election-hacking-1504652957

- **Ransomware:** We've seen massive disruptions to business operations and municipalities through "ransomware," including episodes involving the WannaCry and NotPetya malwares. The most recent attack on Atlanta shut down government operations for over a week. The WannaCry attack ravaged computers at hospitals in England, universities in China, rail systems in Germany, even auto plants in Japan. Additionally, a large pharmaceutical company had 75,000 machines affected by the malware and lost critical research. Incidents like Atlanta, WannaCry, and NotPetya caused massive disruptions to enterprises and municipalities worldwide on an unprecedented scale and indicate a rise in nation-state actors involved in driving these kinds of attacks.

- **Ukraine:** In Ukraine, in 2016 and 2017, there were attacks on the country's energy infrastructure that caused the lights to go out. We've seen similar things in other parts of the world. The most concerning threat to national-security professionals is a devastating attack on critical infrastructure.

- **Russian malware found in critical infrastructure:** Similar to Ukraine, the Trump administration recently accused Russian government hackers of carrying out a deliberate, ongoing operation to penetrate vital US industries, including the energy grid — a major ratcheting up of tensions between the two countries over cybersecurity.[7]

- The Edison Electric Institute reported that its Federal government partners informed energy grid operators in North America of a threat targeting the energy and critical manufacturing sectors. While this incident did not have operational impacts, the group worked across the sector and with government partners to ensure the ongoing protection of the grid from this specific threat and from all cyber and physical security risks. Following the announcement of sanctions against Russian government cyber actors, the Electricity Information Sharing and Analysis Center (E-ISAC) provided potential indicators of compromise and other technical data to ensure electric companies in North America are prepared to protect and defend their networks. This information sharing is representative of the strong industry-government partnership, which exists through the Electricity Subsector Coordinating Council, and is vital to guarding the grid from all possible threats.

- Similarly, following the news of the intrusion, the Department of Energy created a new Office of Cybersecurity, Energy Security, and Emergency Response (CESER) at the US Department of Energy (DOE). $96 million in funding for the office was included in President Trump's FY19 budget request to bolster DOE's efforts in cybersecurity and energy security.[8]

Responding to Today's Threats

Just as the threat environment has evolved, so too must our ability to respond to those threats. This evolution has been most evident within the intelligence community and military, where the National Security Agency (NSA) and United States Cyber Command continue to develop new capabilities designed to counter emerging cyber threats. While this is not the setting in which to focus on these capabilities, I can say that I am confident that the cyber capabilities of the United States are second-to-none. However, I believe there is still work to be done in other areas, particularly in regard to cyber strategy and policy outside of the military and intelligence communities. The two areas of strategy and policy I'd focus on most would be cyber defense and cyber deterrence.

---

[7] *See* https://www.us-cert.gov/ncas/alerts/TA18-074A

[8] See https://www.energy.gov/articles/secretary-energy-rick-perry-forms-new-office-cybersecurity-energy-security-and-emergency

Cyber Defense

The first area of policy that I would address is in cyber defense. How we defend ourselves, and more particularly our cyber infrastructure and networks, is vital to our security and an area in which progress can have a direct impact on minimizing the harms of cyber-attacks. As many in the cybersecurity field have observed, an ounce of prevention is worth a pound of cure.

In order to improve our cyber defenses, it is important to understand how responsibilities for cyber defense are distributed. Within the Federal government these responsibilities are spread among several organizations, so there must be coordination and collaboration on cyber issues between agencies and departments. DOD is responsible for the defense of its networks, while DHS has primary operational responsibility for the defense of all Federal, unclassified civilian networks. Domestic cyber-attack and cyber-crime investigations are the responsibility of the FBI. There is certainly work to be done to fully operationalize these concepts and enhance cybersecurity collaboration within the government so that there is a broader unity of effort within government that helps to grow and enhance our nation's security posture.

In contrast, cybersecurity responsibilities within the private sector are far more diffuse. The security of each network is the responsibility of its owner or operator, meaning that the security of the vast majority of the country's cyber infrastructure is in the hands of hundreds of thousands of different entities. Coordination and information sharing between these entities is often limited, though significant progress has been made in some sectors through the growth of Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs). In this diffuse environment, it is critical that the United States government assist the private sector in their cybersecurity efforts and work diligently to help facilitate critical cybersecurity information sharing, both among private sector actors and between the government and the private sector.

What makes information sharing so important is the fact that our cyber infrastructure is so diffuse. While one entity, such as the FBI, Google, or Microsoft, may be aware of a particular vulnerability or threat, it can take days, weeks, or even months before the relevant information spreads throughout the cyber ecosystem and results in the deployment of patches, installation of new technologies, changes in network architecture, or the adoption of new policies that adequately counter the threat. We have, admittedly, made significant progress in cyber threat information sharing over the past decade. I applaud the efforts of organizations such as the Financial Sector ISAC (FS-ISAC), the Multi-State ISAC (MS-ISAC), and the hundreds of other ISACs and ISAOs that have helped us get to where we are today—but the reality is that we can do more.

On the government side, we already have programs in place that provide the private sector with threat information data and other forms of assistance designed to help private organizations enhance their cybersecurity posture. These programs have had their successes, but it remains too difficult for those in the private sector to gain access to the wealth of information and assistance that the government, particularly DHS, could provide.

For example, DHS's National Protection and Programs Directorate (NPPD) operates the Cyber Information Sharing and Collaboration Program (CISCP), which can be an invaluable source of threat information data for private entities, potentially providing them with access to government threat information data, including sensitive, classified information. However, navigating the process to participate in this program and gain access to classified information can be daunting for private companies. To join the program, the company must first be aware of its existence, and in my experience too few companies are aware of CISCP and other assistance programs offered by

DHS and other government agencies. Once a company is aware of the program, it must then negotiate a Cooperative Research and Development Agreement (CRADA) with DHS, a type of agreement that was not originally designed to facilitate this type of information sharing. The negotiation of a CRADA, while relatively straight forward, can be confusing to companies unfamiliar with government processes or cooperative agreements and can take months to negotiate.

Further, even with a CRADA in place, a company will only have access to less sensitive types of government threat data—classified information remains off limits for a variety of reasons. The data companies do have access can also be incomplete, missing additional, unclassified threat information from agencies outside of DHS, such as the FBI, meaning that a company may need to receive threat information from multiple government entities to receive a more complete picture. To review more sensitive, classified threat information the private company will need to obtain the proper clearances for several of the company's representatives.

Fortunately, DHS can sponsor at least some company personnel for a clearance when a CRADA is in place, but here too are obstacles. The process for obtaining a clearance can be confusing and time consuming, especially for those in the private sector with no previous experience in national security or government service. Further, the Federal government continues to face a significant clearance process backlog. Last month, the Government Accountability Office released a report that found that the Office of Personnel Management's National Background Investigation Bureau currently has a backlog 710,000 background investigation cases, meaning that the entire clearance process can take upwards of a year.[9] Under these circumstances one can understand why a private company might choose to forgo access to more sensitive threat information.

In addition to process improvements, there are ways in which the government can make the threat information data they are already sharing more useful to the private sector. First, threat information sharing is significantly more efficient when it is automated, relying on standardized feeds and formats to communicate key pieces of data. DHS and the government writ-large should continue to encourage the automated sharing of threat information and push for greater interoperability between such initiatives, including the incorporation of confidence levels in the sharing of cyber threat indicators (such as IP addresses and MD5 hashes).

Second, the government should prioritize the identification and sharing of Tactics, Techniques, and Procedures (TTPs) as well as exploit targets for sharing with the private sector. Such information is increasingly important as cyber adversaries rapidly vary traditional signatures used to counter cyber-attacks, such as IP addresses and MD5 hashes. A greater understanding of the TTPs and exploit targets used by an adversary can allow security professionals to focus network hardening and detection efforts to more surgically address risks relevant to their environment, allowing them to prioritize internal controls and policies to match likely threat actor TTPs.

Third, the government should encourage further work on the development of a common language for the exchange of threat information—threat information data is most valuable when all of the organizations involved use the same terminology to describe various TTPs. Within the cyber field there is a significant focus on the Structured Threat Information eXpression (STIX) framework, however many practitioners leverage different frameworks (VERIS, for example) to manage threat TTP and incident information. I would recommend working to resolve the difference between the these various systems with a focus on defining a common language for sharing.

Fourth, the government should foster the collection and categorization of incident data to identify TTPs and other relevant information. A key source of TTP information lies in information collected as part of an incident response

[9] *See* https://www.gao.gov/assets/700/690499.pdf

effort. Thus, there needs to be a greater focus on "reverse engineering" incidents to identify TTPs utilized and corresponding courses of action that could mitigate such TTPs. DHS is currently sponsoring a Cyber Incident & Data Analysis Repository (CIDAR) initiative to define the architecture for an incident repository, however the success of such an initiative will come down to the willingness of organizations to contribute this data. As such, we must do all that we can to encourage companies, in addition to Federal government entities, to share this information in the name of enhancing our collective cybersecurity posture.

To that end, the government should also consider expanding the scope of the Support for Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act to include cybersecurity-related technologies in addition to anti-terrorism technologies. The SAFETY Act, first passed as part of the Homeland Security Act of 2002, provides incentives for the development and deployment of anti-terrorism technologies by creating systems of risk and litigation management. The act provides some terrorism-related liability limitations for organizations that adopt DHS-certified anti-terrorism technologies, creating an incentive for companies to invest and deploy these technologies. Expanding the safety act to include cybersecurity technologies would create a similar incentive for their development and adoption, ultimately encouraging an enhanced cybersecurity posture across the private sector. Legislation to expand the scope of the scope of the SAFETY Act, the Cyber SAFETY ACT of 2018, was recently introduced in the Senate by Senator Steve Daines (R-Montana).

Finally, the private sector has benefited greatly from the National Institute of Standards and Technology's (NIST's) Cybersecurity Framework. This voluntary framework, which consists of standards, guidelines, and best practices for organizations to manage cybersecurity-related risk, has been well received in both the private and public sectors. It has helped organizations prioritize and identify areas deserving of additional investment and attention while promoting the protection and resilience of cyber infrastructure across sectors. That said, NIST can continue to refine and enhance the framework as it continues to iterate and update the document. I would encourage NIST to focus on providing more specific, control-related guidance, providing industry with a clearer understanding of what actions organizations should be taking to implement a control. Such guidance would be in addition to providing references to other cybersecurity frameworks and control regimes as the current framework does.

Cyber Deterrence

The second area of cyber policy and strategy that I would focus on is cyber deterrence. While having the proper policies and technologies in place to defend our cyber infrastructure is important, it is equally important that we have the right tools at our disposal to successfully deter or respond to cyber adversaries from undertaking a cyber-attack in the first place. While we will never be able to deter every cyber-attack, we can use those that do take place to make it clear what responses we have at our disposal and indicate what costs we can inflict on those who undertake such an attack.

The most important question to address when contemplating cyber deterrence is that of attribution. While others testifying before this body are far more qualified to speak to the technical questions of attribution, the broader point remains—attribution of a cyber-attack to a specific actor is vital to providing the United States with the opportunity to use the full range of deterrent options at its disposal. Unfortunately, in the cyber realm attribution can be exceedingly difficult. Attackers can be adept at obfuscating their origins, will leverage tools, vulnerabilities, and TTPs pioneered by others, and leverage the systems of other unsuspecting victims to support and launch their attacks.

We have, fortunately, made significant progress on attribution, though many of the methods and technologies underpinning these capabilities remain highly sensitive. But even our advanced capabilities have limitations—

rarely does a cyber-attack have the sort of indisputable evidence that we have come to expect in the physical world. There may not be a smoking gun or a bloody knife. There won't be a satellite image of our adversary launching their cyber weapon at the United States and rarely is a cyber weapon system something that is exclusive to a single actor. Sometimes the evidence will ultimately come from signals or human intelligence rather than a forensic analysis of the attack itself. The reality is that much of the evidence available to us in the cyber realm is circumstantial, and the confidence level of an attribution can be just as important as the attribution itself.

While not ideal, this is a circumstance that we will ultimately have to come to terms with. We must continue to make investments in our capabilities but will need to rely upon the judgement of our intelligence agencies and technical experts. We may not have the time, or the ability, to wait for complete certainty. We may instead need to identify what level of confidence is needed in what circumstance.

Similarly, we need to ensure that we have a full range of options at our disposal when we respond to a cyber-attack to properly deter future attacks. Like in the physical world, those responses must ultimately be calibrated to the severity of the attack and specifics of the circumstance. As a result, the range of potential responses will range from diplomatic warnings to a proportional cyber response, from a criminal indictment to a kinetic strike on a physical battlefield. We must be prepared to leverage all our options and be certain to properly calibrate their severity to that of the cyber-attack. We must also make it clear that we are willing to use all the options at our disposal.

The criminal indictments obtained by Special Counsel Mueller for 13 Russian nationals and 3 Russian entities are examples of how we can leverage the criminal justice system.[10] The Department of the Treasury's recent targeted sanctions against various Russian national and entities, including 7 Russian oligarchs, similarly demonstrates how we can leverage targeted sanctions.[11] Broader sanctions, including economic and banking sanctions, can also be leveraged as both a response to a cyber-attack and a deterrent against future attacks. Offensive cyber activities and even kinetic military strikes may also be justified in certain circumstances. What is important is that the United States responds in a proportional manner and in one that deters our adversaries from taking similar action in the future.

We must also consider new ways in which we can cooperate and coordinate with our allies on cybersecurity, not just in terms sharing intelligence and capabilities, but in deterrence as well. Toomas Hendrik Ilves, the former President of Estonia and Visiting Fellow at the Hoover Institution at Stanford University, recently proposed what he termed a new "Cyber NATO," a coalition of liberal democracies that is better able to meet the ubiquity of cyber threats and ensure proper, adequate response.[12] The President of Microsoft, Brad Smith, has proposed what he has dubbed a "Digital Geneva Convention," which outlines the rules of cyberspace and protects civilians and other bystanders from the offensive cyber activities of nation-states.[13] These are the sorts of bigger ideas that we must also consider as the volume of cyber-attacks grows and our capabilities mature.

Conclusion

The size and scope of state-sponsored threats facing the US may seem daunting and it is important for us to recognize that we are unable to prevent all attacks. But altering our cyber defense and deterrence strategies will

---

[10] ***See*** https://www.justice.gov/file/1035477/download

[11] ***See*** https://home.treasury.gov/news/press-releases/sm0312 and https://home.treasury.gov/news/press-releases/sm0338

[12] ***See*** https://berlinpolicyjournal.com/a-digital-defense-alliance/

[13] ***See*** https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

go a long way toward mitigating the risk. Congress must act to address the shortcomings of the current security clearance process, consider expanding the scope of the SAFETY Act to include cybersecurity-related technologies to incentivize private sector companies to create innovative defense technologies, and simplify and standardize information sharing between the private and public sectors to ensure that it is easier for enterprises to share and receive threat information from the government in real time. Thank you to the Committee Chairman for inviting me to testify today. This hearing is a positive step in helping our country better defend against and deter cyber-attacks.

Michael Chertoff
Chairman & Founder

Chertoff Group, LLC
1110 Vermont Avenue, NW
Suite 1200
Washington, D.C. 20005

Michael Chertoff is Chairman & Founder of the Chertoff Group, a security and risk management advisory firm with offices in Washington, D.C., New York, and Menlo Park. He is the Chairman of the Board of Directors of BAE Systems, Inc., the U.S.-based subsidiary of BAE Systems plc. Judge Chertoff is also senior of counsel at Covington & Burling and is the Co-Chair on the Global Commission on the Stability of Cyberspace

Most recently, Mr. Chertoff served as Secretary of the Department of Homeland Security. As Secretary, he led a 218,000 person department with a budget of $50 billion. Mr. Chertoff developed and implemented border security and immigration policy; promulgated homeland security regulation; and spearheaded a national cyber security strategy. He also served periodically on the National Security and Homeland Security Councils, and on the Committee on Foreign Investment in the United States.

Prior to his appointment to the Cabinet, Mr. Chertoff served from 2003 to 2005 on the U.S. Court of Appeals for the Third Circuit. Before becoming a federal judge, Mr. Chertoff was the Assistant Attorney General for the Criminal Division of the U.S. Department of Justice. In that position, he oversaw the investigation of the 9/11 terrorist attacks, and formed the Enron Task Force, which produced more than 20 convictions, including those of CEOs Jeffrey Skilling and Kenneth Lay.

Mr. Chertoff's career includes more than a decade as a federal prosecutor, including service as U.S. Attorney for the District of New Jersey, First Assistant U.S. Attorney for the District of New Jersey, and Assistant U.S. Attorney for the Southern District of New York. As a federal prosecutor, Mr. Chertoff investigated and personally prosecuted significant cases of political corruption, organized crime, and corporate fraud.

From 1994-2001, Mr. Chertoff represented major corporations and individuals in numerous white collar investigations and trials. Among other matters, he successfully represented the nation's largest hospital company in a four year, multi-jurisdictional criminal and civil investigation, represented major corporations in corruption scandals, and obtained acquittals at trial for individual criminal defendants.

Mr. Chertoff has received numerous awards including the Department of Justice Henry E. Petersen Memorial Award (2006); the Department of Justice John Marshall Award for Trial of litigation (1987); NAACP Benjamin Hooks Award for Distinguished Service (2007); European Institute Transatlantic Leadership Award (2008); and two honorary doctorates. His trial experiences have been featured in over half a dozen books and many news articles.

Education

- Harvard Law School, J.D., 1978
  - *magna cum laude*
- Harvard College, B.A., 1975
  - *magna cum laude*

Clerkships

- Hon. William Brennan, Jr., U.S. Supreme Court, 1979-1980
- Hon. Murray Gurfein, U.S. Court of Appeals, Second Circuit, 1978-1979

Bar Admissions

- District of Columbia
- New York
- New Jersey

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the U.S. House of Representatives for the 115th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), or contracts or payments originating with a foreign government, received during the current and two previous calendar years either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. This form is intended to assist witnesses appearing before the House Committee on Armed Services in complying with the House rule. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number) will be made publicly available in electronic form not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary.

Witness name: Michael Chertoff

Capacity in which appearing: (check one)

☒ Individual

☐ Representative

If appearing in a representative capacity, name of the company, association or other entity being represented: _____

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, please provide the following information:

2018

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

2017

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

2016

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

Foreign Government Contract or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or payments originating from a foreign government, please provide the following information:

2018

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment

2017

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment

2016

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment

Prepared Statement of GEN (Ret) Keith B. Alexander*
on
Cyber Warfare Today: Preparing for 21st Century Challenges
in an Information-Enabled Society
before the
House Armed Services Committee

April 11, 2018

Chairman Thornberry, Ranking Member Smith, Members of the Committee: thank you for inviting me to discuss the current threats and challenges that we face as a nation in cyberspace and how we might modify our current policies to address these problems. I applaud you both for approaching these issues in a bipartisan, strategic manner and for the series of hearings and briefings that today's panel kicks off. I know that you will hear later today from some of our government's leaders in this area in both an open and closed setting and that you'll be focused on operational and budgetary matters in upcoming sessions, so my plan today is to set out some of the larger trends and issues that I see facing our nation and to put on the table some initial ideas about how these issues might be addressed.

Mr. Chairman, as you know, I've long been an advocate for the view that in the modern era of threats that face our nation, we must fundamentally rethink our nation's architecture for cyber defense. Today we face strategic threats in cyberspace from two nations that have long been our key adversaries in this domain: China and Russia. We also face tactical threats from a range of actors, including increasingly active nation-states like North Korea and Iran, as well as wide array of non-state actors from criminal gangs to terrorist groups. And some of these latter actors are working on behalf of, or alongside, the nation-states that are also operating against us in the cyber domain.

And while we increasingly recognize these threats as a nation, and as our government becomes more open and robust about calling out those who would threaten our national security, we still remain overly cautious about making hard decisions regarding the appropriate roles and responsibilities of the government and the private sector. Even as our nation maintains the lead in technological innovation and builds our economy based in significant part on growth in the technology sector, I worry that we are not yet ready as a nation to grapple with the reality that cyberspace has become a domain for warfare and that we very much are in the throes today of a series of ongoing—albeit currently low-level—conflicts in cyberspace.[1]

---

* Gen. (ret.) Keith B. Alexander is the former Director, National Security Agency and Founding Commander, U.S. Cyber Command. Gen. Alexander currently serves as President and CEO of IronNet Cybersecurity, a startup cybersecurity firm and in a range of other capacities in the public and private sectors. Gen. Alexander is testifying before this Committee today in his personal, individual capacity.

[1] *See, e.g.*, Office of the Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community*, at 5-6 (Mar. 6, 2018) ("The risk is growing that some adversaries will conduct cyber attacks—such as data deletion or localized and temporary disruptions of critical infrastructure—against the United States in a crisis short of war....Russia, China, Iran, and North Korea will pose the greatest cyber threats to the United States during the next year. These states are using cyber operations as a low-cost tool of statecraft, and we assess that they will work to use cyber operations to achieve strategic objectives unless they face clear repercussions for their cyber operations.... The use of cyber attacks as a foreign policy tool outside of military conflict has been mostly limited to

The recent National Security Strategy (NSS) released by the White House makes clear what we have long known: economic security is national security.[2] As the NSS makes clear, "[a] strong economy protects the American people, supports our way of life, and sustains American power…[and a] growing and innovative economy allows the United States to maintain the world's most powerful military and protect our homeland."[3] At the same time, we've long known that our economic security is being challenged directly in cyberspace by nations, like China, that continue to siphon off massive amounts of economic wealth through the theft and coerced transfer of the very intellectual property that is at the heart of our modern economy.[4]

Our national security is even more directly threatened by nations like Russia who have engaged in obvious efforts to undermine confidence in our political system,[5] have sought to put in place long-term penetrations in critical infrastructure sectors in order to conduct espionage and prepare the battlespace for potential future conflict scenarios,[6] and have conducted what our government recently referred to as the most "destructive and costly cyber-attack in history."[7]

---

sporadic lower-level attacks. Russia, Iran, and North Korea, however, are testing more aggressive cyber attacks that pose growing threats to the United States and US partners."), *available online at* <https://www.dni.gov/files/documents/Newsroom/Testimonies/Final-2018-ATA---Unclassified---SASC.pdf>

[2] The White House, *National Security Strategy of the United States of America* at 17 (Dec. 2017), *available online at* <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

[3] *Id.*

[4] *See, e.g.*, The White House, *Remarks by President Trump at Signing of a Presidential Memorandum Targeting China's Economic Aggression* (Mar. 22, 2018) (statement of U.S. Trade Representative Robert Lighthizer) ("Lighthizer:… Technology is probably the most important part of our economy. There's 44 million people who work in high-tech knowledge areas. No country has as much technology-intensive industry as the United States. And technology is really the backbone of the future of the American economy….And we concluded that, in fact, China does have a policy of forced technology transfer; of requiring licensing at less than economic value; of state capitalism, wherein they go in and buy technology in the United States in non-economic ways; and then, finally, of cyber theft."), *available online at* <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-signing-presidential-memorandum-targeting-chinas-economic-aggression/>.

[5] *See, e.g.*, U.S. Department of Treasury, *Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks* (Mar. 15, 2018) ("Today's action counters Russia's continuing destabilizing activities, ranging from interference in the 2016 U.S. election to conducting destructive cyber-attacks, including the NotPetya attack, a cyber-attack attributed to the Russian military on February 15, 2018 in statements released by the White House and the British Government."), *available online at* <https://home.treasury.gov/news/press-releases/sm0312>.

[6] *See, e.g.*, Department of Homeland Security, *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors* (Mar. 15, 2018), ("This alert provides information on Russian government actions targeting U.S. Government entities as well as organizations in the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors….DHS and FBI characterize this activity as a multi-stage intrusion campaign by Russian government cyber actors who targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the Russian government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems (ICS)."), *available online at* <https://www.us-cert.gov/ncas/alerts/TA18-074A>; *see also Worldwide Threat Assessment*, *supra* at n. 1 ("In the next year, Russian intelligence and security services will continue to probe US and allied critical infrastructures, as well as target the United States, NATO, and allies for insights into US policy.").

[7] The White House, *Statement from the Press Secretary* (Feb. 15, 2018) ("In June 2017, the Russian military launched the most destructive and costly cyber-attack in history….The attack, dubbed 'NotPetya,' quickly spread

And these threats don't even account for the fact that our government has recently called out similar IP theft and destructive attacks by both Iran[8] and North Korea.[9]

At the same time, even though we are currently in the middle of a very real series of (minor) military skirmishes in cyberspace, and even though our Constitution has made clear for over 200 years that one of the core missions of the federal government is to provide "for the common defence,"[10] we remain woefully underprepared as a nation to provide effectively for such defense in the cyber domain.

This is not to say we don't have the forces or capabilities in place to do so. The creation of U.S. Cyber Command under my watch within the Department of Defense, with the strong support of this Committee and its members, as well as Cyber Command's continued close work with the National Security Agency, the world's premiere signals intelligence agency, provides our nation with very real and robust capabilities in both the offensive and defensive areas, capabilities that have the ability both protect our nation writ large and to make cyber deterrence a reality in the global arena.

However, the problem is not fundamentally one of force structure at this point. It is one of roles, responsibilities, authorities, and relationships. And on this account, there remains a great deal more to be done. While this Committee has leaned forward and pressed the Department to think more actively about its capabilities, authorities, and warfighting doctrine when it comes to the cyber domain, I remain concerned that we have not yet really grappled with two major issues when it comes to the defense of the nation in cyberspace: (1) how we organize ourselves as a government to defend, fight, and win in this domain; and (2) how we build real jointness between the public and private sectors in what is inevitably going to be a conflict that requires

---

worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas.") *available online at* <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/>.

[8] *See, e.g.*, Department of Justice, *Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps* (Mar. 23, 2018 (describing Iranian hackers that "conducted a coordinated campaign of cyber intrusions into computer systems belonging to 144 U.S. universities, 176 universities across 21 foreign countries, 47 domestic and foreign private sector companies, the U.S. Department of Labor, the Federal Energy Regulatory Commission, the State of Hawaii, the State of Indiana, the United Nations, and the United Nations Children's Fund."), *available online at* <https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary>; *see also Worldwide Threat Assessment*, *supra* at n. 1 at 6 ("Iran's cyber attacks against Saudi Arabia in late 2016 and early 2017 involved data deletion on dozens of networks across government and the private sector."), *available online at* <https://www.dni.gov/files/documents/Newsroom/Testimonies/Final-2018-ATA---Unclassified---SASC.pdf>.

[9] *See, e.g.*, The White House, *Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea* (Dec. 17, 2017) ("In May of this year, a dangerous cyberattack known as WannaCry spread rapidly and indiscriminately across the world. The malware encrypted and rendered useless hundreds of thousands of computers in hospitals, schools, businesses, and homes in over 150 countries….This was a careless and reckless attack. It affected individuals, industry, governments. And the consequences were beyond economic. The computers affected badly in the UK and their healthcare system put lives at risk, not just money. After careful investigation, the United States is publicly attributing the massive WannaCry cyberattack to North Korea."), *available online at* <https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/>.

[10] *See* U.S. Const., preamble.

both the government and industry to act with speed and vigor if we are going to truly be able to defend the nation.

Over half a decade has passed since 2012, when then-Secretary of Defense Leon Panetta made clear that it is the U.S. government's policy that "the Department [of Defense] has a responsibility…to be prepared to defend the nation and our national interests against an attack in or through cyberspace"[11] and this year's National Defense Strategy highlights the importance of providing such defense, noting that

> It is now undeniable that the homeland is no longer a sanctuary. America is a target, whether from terrorists seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion…[And the] increasing digital connectivity of all aspects of life, business, government, and military creates significant vulnerabilities.[12]

And yet, as this Committee all too well knows, the reality is that today, U.S. Cyber Command lacks the clear authorities and rules of engagement to make this policy effective. While many are rightly concerned with providing authorities prior to the beginning of a conflict, the reality is that in this domain, more than others, we need to ensure that our warfighters can act with speed and agility when the enemy strikes. And structured properly, with appropriate civilian oversight, reporting to Congress, and additional authorizations, the government can effectively mitigate any major concerns with providing such authority now. Indeed, given the potential for overreach, there are significant benefits to working together now, in a bipartisan manner, to provide U.S. Cyber Command with the appropriate authorities and key rules of engagement (ROE) in the relative calm of the current moment rather than making policy in the maelstrom of an ongoing crisis.

But simply providing Cyber Command with robust authorities and solid ROE is not enough. The reality today is that the vast majority of American cyber infrastructure is owned and operated by the private sector and, as a nation, we do not want the government to maintain a long-term, active presence on private sector networks to provide defensive capabilities. As a result, it is critical that that government works closely with the private sector in three areas: (1) setting the conditions for a truly defensible cyber infrastructure; (2) significantly empowering private sector defensive capabilities; and (3) providing for interoperable capabilities and joint exercises in the event that a national crisis requires the government to assist the private sector in a more direct manner or to respond directly against a threat to the nation.

To set the conditions for a truly defensible cyber infrastructure, we must recognize a basic fact about the cyber threat environment today: namely that no single entity—whether a private sector company or a government agency—can stand alone against the most capable threat actors.

---

[11] *See* Department of Defense, *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City* (Oct. 11, 2012), available online at <http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136> .

[12] *See* Department of Defense, *Summary of the 2018 National Defense Strategy* (Jan. 19, 2018), at 3, *available online at* <https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

Indeed, in no other area do we expect individual private companies to defend themselves against nation-states. For example, while we reasonably expect Target to have high fences and armed guards around its warehouses to protect against thieves, we surely don't expect Target or Walmart or any other American company to have surface-to-air missiles on the roofs of those warehouses to defend against the threat of a Russian bomber dropping munitions.[13] And yet today, when it comes to cyberspace, we expect exactly that. This policy simply makes no sense; expecting individual companies, standing alone, to defend themselves against all comers, including nation-states—which, to be fair, is our current expectation—is a policy designed to fail.

Instead, as a nation, we need to move to a collective defense architecture both within the private sector, as well as between the public and private sectors. The good news is that we have already taken significant steps in this direction, with various sectors creating information sharing and analysis centers and organizations (ISACs/ISAOs) and the government crafting legislation to encourage information sharing amongst companies as well as with the government. The reality, however, is that even with these organizations in place, we still have yet to create the right incentives to share information at scale and speed within the private sector and with the government.[14] To be sure, some sectors, like the energy and financial sectors, are beginning to lead in this space. But more remains to be done, both as a matter of policy as well as authorities. We must increasingly think of our critical industries not just as a coalition of key companies and sectors, but as a set of strategic assets that require a combined, joint arms effort to defend them. Much good intellectual work has been done in this space including: (1) discussions about creating and empowering a Strategic Infrastructure Coordinating Council (SICC);[15] (2) the extremely valuable and practical recommendations of the National Infrastructure Advisory Council (NIAC);[16] and (3) the notion of creating a public-private advisory body to the National Security Council (NSC) in the form of the National Cybersecurity Public-Private Partnership

---

[13] *See, e.g.*, Keith B. Alexander, et. al, *Clear Thinking About Protecting the Nation in the Cyber Domain*, 2 Cyber Defense Review 29, 33 (No. 1) (2017) ("The fact is that commercial and private entities cannot be expected to defend themselves against nation-state attacks in cyberspace. Such organizations simply do not have the capacity, the capability, nor the authority to respond in a way that would be fully effective against a nation-state attacker in cyberspace. Indeed, in most other contexts, we do not (and should not) expect corporate America to bear the burden of nation-state attacks. For example, we do not expect Target to employ surface-to-air missiles to defend itself against Russian planes dropping bombs in the United States. Rather, that responsibility belongs to the DoD. Today, however, in cyberspace, that expectation is flipped on its head.")

[14] *See* Keith B. Alexander, *Prepared Statement on Cyber Strategy and Policy before the Senate Armed Services Committee* (Mar. 2, 2017) ("The cyber legislation enacted by Congress last year is a step in the right direction; however, it lacks key features to truly encourage robust sharing, including placing overbearing requirements on the private sector, overly limiting liability protections, restricting how information might effectively be shared with the government, and keeping the specter of potential government regulation looming in the background"), available online at <https://www.armed-services.senate.gov/imo/media/doc/Alexander_03-02-17.pdf>.

[15] *See, e.g.*, Electricity Subsector Coordinating Council, *ESCC Initiatives* (Jan. 2018), *available online at* <http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8>.

[16] *See, e.g.*, Department of Homeland Security, National Infrastructure Advisory Committee, *Securing Cyber Assets: Addressing Urgent Threats to Cyber Infrastructure*, at 3-4, 7-20 (Aug. 2017), *available online at* <https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf>

(NCP3),[17] as recommended by a recent Presidential commission that I served on alongside key individuals from the private sector including the former CEO of IBM, Sam Palmisano, and the CEO of Mastercard, Ajay Bangha. But the time for purely intellectual exercises has passed; it is now critical that we begin taking the right steps to implement these ideas in practice.

When it comes to empowering private sector defensive capabilities, here too the government can and should do more. For far too long the government has talked about the need to share threat information at speed and scale with the private sector. But continued talk will mean little if the day comes to pass where the government knew of a major threat to the American private sector that it could have helped defend against and but didn't share it in an actionable form, in real-time. The government must be prepared not only to share declassified information with the private sector in real-time and at machine-speed, but also must be prepared to use its overseas intelligence collection architecture to collect on threats to the American private sector and to pass on this information—even in its highly classified form—to the private sector, so that it may be utilized to defend industry. Similarly, if the nation is to become truly defensible, the government must work with industry to develop a cyber common operational picture, analogous to the air traffic control picture. Just as the air traffic control picture ensures aviation safety and helps synchronizes government and civil flights, a cyber common operational picture can help synchronize our national common cyber defense and enable rapid response in a time of crisis.

Finally, the government and industry ought to work together to develop interoperable capabilities that can be utilized in a crisis and to exercise these capabilities in advance of an actual threat. Such efforts, as recommended by the NIAC,[18] will allow the nation to have a plan and capability in place should the need arise in case of an actual cyber conflict scenario.

As a former commander of forces deployed around the world, I also feel strongly that unity of command is critical. Today we divide responsibility for the ongoing, day-to-day defense of the government amongst various agencies, including Cyber Command and DHS. We likewise divide responsibility for private sector outreach and collaboration on cyber defensive efforts between Cyber Command, DHS, and FBI. To that end, it is my view that in the time of a crisis, all of these capabilities have got to come under a single authority. And while I know this will be a hotly debated recommendation—not to mention where the authority ought to reside—the reality is that while we have gotten away for a quite a while with various agencies stepping on one another's toes, more must be done going forward to get the government working more closely together if we are to be able to respond effectively in a crisis scenario. At a minimum, as the government debates and discusses the wisdom of such a larger effort, at least within the White House, the President ought to immediately elevate existing roles by appointing an Assistant to the President for Cybersecurity who reports to the President through the National Security Advisor and charge that individual with leading national cybersecurity policy and

---

[17] *See, e.g.*, Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy* (Dec. 1, 2016), at 14-15, *available online at* <https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf>.

[18] *See, e.g.*, Department of Homeland Security, National Infrastructure Advisory Committee, *Securing Cyber Assets: Addressing Urgent Threats to Cyber Infrastructure*, at 8-9, 18 (Aug. 2017), *available online at* <https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf>

coordinating implementation of the nation's cyber protection program and taking input from the recommended NCP3.

In sum, Mr. Chairman, I think much remains to be done to create a truly defensible national cyber architecture. But I believe that we can get there, particularly with the support of this Committee and its leadership, reaching across the aisle to solve this truly national problem. I stand ready to assist you, the Ranking Member, and the other members of this Committee and your staff to work on this effort. Thank you to both you and the Ranking Member for your leadership and for holding this hearing. I am prepared to answer any questions you or the members of the Committee may have.

Keith Alexander
Founder & CEO
IronNet Cybersecurity

At IronNet Cybersecurity, as the CEO and President, General (Ret) Keith Alexander provides strategic vision to corporate leaders on cybersecurity issues through development of cutting-edge technology, consulting and education/training. He is reinventing how industries mitigate cybersecurity threats with IronDefense, a patented solution designed to detect and alert on anomalous enterprise network behaviors through fine-tuned analytics. His goal is to bridge communication systems between private and government sectors to create the next level of intelligence sharing and protect the nation against cyber threats on a global stage.

General Alexander is a four-star general with an impressive 40-year military career, culminating in role of the Director of the National Security Agency (NSA) and Chief of the Central Security Service (CSS) from 2005-2014. He holds the distinction of serving in this role longer than any other director. While serving as the NSA Director, he was appointed by Congress to be the first Commander to lead the U.S. Cyber Command (USCYBERCOM). He held this role from 2010-2014, establishing and defining how our nation is protected against cyber attacks.

As Commander, USCYBERCOM, General Alexander was responsible for planning, coordinating and conducting operations, and defending Department of Defense (DoD) computer networks—as well as the defense of the nation—from cyber threats. As the Director of NSA, he was responsible for national foreign intelligence requirements, military combat support, and the protection of U.S. national security information systems.

Prior to leading USCYBERCOM and the NSA/CSS General Alexander served as the Deputy Chief of Staff, Intelligence, Department of the Army; Commanding General of the U.S. Army Intelligence and Security Command at Fort Belvoir, VA; and the Director of Intelligence, United States Central Command, MacDill Air Force Base, FL., and the Deputy Director for Requirements, Capabilities, Assessments and Doctrine, J-2, on the Joint Chiefs of Staff.

Serving as a member of the President's Commission on Enhancing National Cybersecurity, General Alexander developed key recommendations to create a defensible national cyber architecture to protect national security by promoting rapid innovation and close public-private collaboration while preserving privacy and civil liberties.

General Alexander is the recipient of the 2016 United States Military Academy (USMA) Distinguished Graduate Award. He holds a BS from the U.S. Military Academy, as well an MS in Business Administration from Boston University; an MS in Systems Technology and an MS in Physics from the Naval Post Graduate School; and an MS in National Security Strategy from the National Defense University.

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the U.S. House of Representatives for the 115th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), or contracts or payments originating with a foreign government, received during the current and two previous calendar years either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. This form is intended to assist witnesses appearing before the House Committee on Armed Services in complying with the House rule. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number) will be made publicly available in electronic form not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary.

Witness name: Gen. (ret.) Keith B. Alexander

Capacity in which appearing: (check one)

☒ Individual

☐ Representative

If appearing in a representative capacity, name of the company, association or other entity being represented: N/A

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, please provide the following information:

2018

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
N/A			

2017

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
N/A			

2016

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
N/A			

Foreign Government Contract or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or payments originating from a foreign government, please provide the following information:

2018

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
N/A			

2017

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
N/A			

2016

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
N/A			

FINAL

Prepared Statement of Jeh Charles Johnson
Before the House Armed Services Committee
Hearing on *"Cyber Operations Today: Preparing for 21st Century Challenges in an Information-Enabled Society"*
April 11, 2018

Chairman Thornberry, Ranking Member Smith and members of this Committee:

From February 10, 2009 to December 31, 2012, I served as General Counsel of the Department of Defense. From December 23, 2013 to January 20, 2017, I served as Secretary of Homeland Security. As Secretary, I had the privilege of working with Congress to provide additional authorities to the Department of Homeland Security to defend the Nation's and the federal government's cybersecurity, through the Cybersecurity Act of 2015,[1] the National Cybersecurity Protection Act of 2014,[2] the Federal Information Security Modernization Act of 2014,[3] and other new laws.[4]

I am pleased the Committee has convened this hearing on the important topic of cyber operations and cybersecurity, and I'm pleased to be joined at the witness table by Secretary Chertoff and General Alexander. The views I express here are my own, based upon my personal experiences in national security and, now, as a concerned private citizen.

You have asked the witnesses today to focus our testimony on the following:

> *[T]he current cybersecurity challenges and threats to U.S. military superiority being posed by Russia, China and other state-sponsored actors aggressively engaged in the cyber domain conducting activities to enable information warfare below the traditional level of armed conflict. Please also discuss policy and capabilities with respect to current U.S. plans and strategies, including ways to improve interagency coordination for cyber threats. Lastly, we ask*

[1] Pub. L. No. 114-113, 129 Stat. 2242, 2935 (2015).
[2] Pub. L. No. 113-282, 128 Stat. 3066 (2014).
[3] Pub. L. No. 113-283, 128 Stat. 3073 (2014).
[4] *E.g.*, the Border Patrol Agent Pay Reform Act of 2014, Pub. L. No. 113-277, 128 Stat. 2995 (2014) (including additional authorities for cybersecurity recruitment and retention).

that you recommend ways and means to better prepare for 21st century challenges in an information-enabled society by improving the organization of the U.S. government.

The Threat Picture

Cyberattacks on our homeland, of all manner and from multiple sources, are going to get worse before they get better. In this realm and at this moment, those on offense have the upper hand; those on defense struggle to keep up. Whether nation-state actors or non-state cyber-criminals, hacktivists, or those who engage in the growing industry of Ransomware, those on offense are ingenious, tenacious, agile, and getting better all the time.

To understand the current cybersecurity threats to our homeland from nation-states and others, we must, in my view, divide them into five broad threat streams:

First, the threat of cyberattack by a nation-state or other entity to seize, disable, or destroy components of our Nation's critical infrastructure. This form of cyberattack implicates national security, and, if significant enough in its effects, may amount to an act of war.[5] This form of cyberattack may also occur as part

[5] A key question many ask is: under what circumstances can a cyberattack constitute an act of war? At the moment, there is no legal definition for the term "cyberwar." The 1022-page Department of Defense Law of War Manual, which was published in 2015 and took decades, literally, to write, contains a section on cyber operations, but does not contain a definition of the term cyberwar or take on the question of when a cyberattack constitutes an act of war, justifying an armed response. On this issue, I agree with the existing assessments from legal scholars I have come to know and trust, Professors Jack Goldsmith (Harvard Law) (Jack Goldsmith, *How Cyber Changes the Laws of War*, 24 EUR. J. INT'L L. 129 (2013)); Oona Hathaway (Yale Law) (Oona Hathaway, *et al., The Law of Cyber Attack*, 100 CAL. L. REV. 817 (2012)) and Major General (ret) Charles Dunlap (Duke Law) (Charlie Dunlap, *Are Cyber Norms as to What Constitutes an "Act of War" Developing as We Would Want?*, LAWFIRE (Sept. 15, 2017), https://sites.duke.edu/lawfire/2017/09/15/are-cyber-norms-as-to-what-constitutes-an-act-of-war-developing-as-we-would-want/), among others.

Essentially, the answer from them, and me, is "maybe," or "it depends," or "we will know it when we see it."

The experts recognize that the terms "use of force" and "armed attack" are hard to translate into the cyber realm. However, the consensus view calls for an analysis of the kinetic effects of an attack, not just the kinetic means. That is, a cyberattack that causes serious kinetic effects, such as the explosive destruction of an air field or an electric grid, and/or physical death and injury (as opposed to cyber espionage or cyber theft of data), should almost certainly be considered an act of war. This is a simple, common-sense approach to the issue. In my judgment, it is not in the interest of the United States to reach for a more creative or expansive definition. An enlarged definition of a cyber "act of war" could be invoked by other nations unilaterally as a justification for an armed response under Article 51 of the UN Charter, or

and parcel of an ongoing armed conflict that has begun in a traditional kinetic fashion.

Second, cyber espionage, practiced principally by nation-states, and similar in purpose to forms of traditional espionage.

Third, hacking and unwanted exfiltration and theft of data and intellectual property. As General Alexander notes in his prepared statement, the theft of intellectual property by nation-states is a significant part of this threat stream. As we saw in 2016, this threat stream also includes, but is hardly limited to, the risk of attack on election infrastructure by nation-state actors, which represents a threat to our very democracy.

Fourth, the problem of widespread use and misuse, but not necessarily theft, of personal, private data on the internet. The reality is that the American public has surrendered and entrusted much of our private lives to the internet. Technically with consent, but often without our knowledge, much of this private data is shared for marketing and commercial purposes, and there is now a growing industry of data mining companies, data brokers, and data intelligence companies dedicated to further exploiting this target-rich environment. Because of its prevalence on the internet, private information is now discoverable and exploitable not only by conventional actors, but by criminal hackers and nation-states. Consequently, this is not just an issue of privacy; it is an issue of security.

Fifth, and finally, the problem that can be considered a form of cyberattack, but not exclusively so – fake news and hateful, extreme views published and republished on the internet, used as a weapon by foreign and domestic forces seeking to alter elections, sow discord, or otherwise alter public opinion generally. The recent indictment of 13 Russian individuals by the Special Counsel[6] confirms that this was part of the Russian attack against us in 2016.

---

for invocation of Article 5 of the NATO treaty. Mistakes in attribution—for which there is an enhanced concern in the cyber realm—could also complicate matters.

This is not meant to imply that the U.S. should not formulate a comprehensive strategy for these attacks—to the contrary, we must continue to develop a set of international rules and norms of acceptable behavior in cyberspace, and the United States should lead that effort.

[6] Indictment, *United States v. Internet Research Agency LLC et al.*, No. 18-cr-00032-DLF, (D.D.C. Feb. 16, 2018), ECF No. 1.

Roles, Responsibilities, and Capabilities

There are vital roles for the U.S. military, the intelligence community, law enforcement, and the Department of Homeland Security in the U.S. government's cybersecurity efforts.

Broadly speaking, the Department of Defense should be responsible for defending the Nation against attacks, and securing national security and military systems; the Department of Justice should be the lead agency responsible for investigating[7] and prosecuting cybercrimes, and the lead agency for domestic national security operations; and DHS should be the lead agency for protection, prevention, mitigation, and recovery when it comes to domestic private and government cyber incidents, as well as securing federal civilian networks. (In addition, the head of each federal agency is responsible for the immediate security of his or her own agency's particular network.)

As between DOJ and DHS, I concur with the approach taken in Presidential Policy Directive 41,[8] which specifies that DOJ is the lead agency for "threat response" (*i.e.*, law enforcement and national security investigations) to significant cyber incidents and DHS is the lead agency responsible for "asset response" (*i.e.*, patching vulnerabilities, forensics, and technical assistance) to significant cyber incidents.

I also support efforts to reorganize DHS internally to more effectively address current cyber threats. There should be a cybersecurity agency of the U.S. government. DHS's current "National Protection and Programs Directorate" should be reorganized into a leaner and more efficient "Cyber and Infrastructure Security Agency" that has two key missions, cybersecurity and infrastructure protection, and recognizes the interconnectivity of these two missions. I support legislative efforts to accomplish these goals.[9]

---

[7] In addition to the FBI, the Secret Service and Homeland Security Investigations have considerable expertise and experience in investigating cybercrimes.

[8] Presidential Policy Directive 41, United States Cyber Incident Coordination (2016).

[9] *See* Cybersecurity and Infrastructure Security Agency Act of 2017, H.R. 3359 (115th Cong.) (2017), passed by the House in December 2017, and Department of Homeland Security Reauthorization Act, H.R. 2825 (115th Cong.) (2017), reported out of the Senate Homeland Security and Governmental Affairs Committee and pending in the Senate.

As for the relative roles in cybersecurity between U.S. Cyber Command and NSA, I defer to the views of General Alexander.

Inevitably, given its nature, cyber security must also be a public-private partnership. As General Alexander notes in his prepared statement, the vast majority of our Nation's cyber infrastructure is owned and operated by the private sector.

In 2015, DHS established near-real-time automated information sharing capability with the private sector. Through the Cybersecurity Act of 2015, Congress provided further incentives for the private sector to share cyber threat indicators with DHS. As of the time I left office, however, not enough businesses had taken advantage of automated information sharing capability. No matter how sophisticated a company's cybersecurity is, everyone benefits from information sharing about the latest cyber threats. The federal government should focus on strengthening partnerships with the private sector, to ensure better information sharing.

By contrast, in my judgment, addressing the problem of fake news and extremist views is not a matter for the security agencies of our government. Foreign influence in federal elections is a matter for the federal election laws, and activities that violate criminal laws are a matter for law enforcement. Beyond that, we must be extremely careful not to go down the road of empowering security agencies to regulate or restrict speech, particularly political speech, on the suspicion that it might have a foreign or extremist origin. Self-regulation by private internet access providers should be the first solution. And the public should be more skeptical about what we read and see.

To meet all of these demands, continued U.S. government investments in both cyber talent and technology are key. I am pleased that the President's FY2019 budget proposes significant amounts for DHS's Continuous Diagnostics and Mitigation Program, and continued deployment of the EINSTEIN system to protect federal civilian networks. The recruitment and retention of cybersecurity talent is perhaps the biggest cybersecurity challenge for DHS and other federal agencies.

Beyond that, I agree with Secretary Chertoff's prepared statement that the U.S. government must define a cyberwarfare doctrine, develop clear guidelines for determining attribution, and continue to incentivize public-private information sharing and investments by the private sector in cybersecurity.

I am prepared to discuss further my own views on these topics, and I look forward to your questions.

Jeh Charles Johnson

Jeh Johnson is the former U.S. Secretary of Homeland Security. He served in that position from December 2013 to January 2017. Johnson now practices law at Paul, Weiss, Rifkind, Wharton & Garrison, LLP. Johnson has been affiliated with Paul, Weiss on and off since 1984, and first became a partner in 1994. Johnson is also currently on the board of directors of Lockheed Martin and the Center for a New American Security.

As Secretary of Homeland Security, Johnson was the head of the third largest cabinet department of the U.S. government, consisting of 230,000 personnel and 22 components, including TSA, Customs and Border Protection, Immigration and Customs Services, U.S Citizenship and Immigration Services, the Coast Guard, the Secret Service, and FEMA. Johnson's responsibilities as Secretary included counterterrorism, cybersecurity, aviation security, border security, port security, maritime security, protection of our national leaders, the detection of chemical, biological and nuclear threats to the homeland, and response to natural disasters. In three years as Secretary of DHS, Johnson is credited with management reform of the Department which brought about a more centralized approach to decision-making in the areas of budgets, acquisition and overall policy. Johnson also raised employee morale across the Department, reflected in the September 2016 Federal Employee Viewpoint Survey.

Prior to becoming Secretary of Homeland Security, Johnson was General Counsel of the Department of Defense (2009-2012). In that position, Johnson is credited with being the legal architect for the U.S. military's counterterrorism efforts in the Obama Administration. In 2010, Johnson also co-authored the report that paved the way for the repeal of the Don't Ask, Don't Tell by Congress later that year. In his book Duty, former Secretary of Defense Robert Gates wrote that Johnson "proved to be the finest lawyer I ever worked with in government – a straightforward, plain-speaking man of great integrity, with common sense to burn and a good sense of humor." In his final days as General Counsel of the Defense Department, Johnson made the first of three appearances at Oxford, this one an address entitled "How Will the War Against al Qaeda End?" The address received international attention and acclaim.

In October 1998, Johnson was appointed by President Clinton to be General Counsel of the Department of the Air Force, and served in that position until January 2001. Earlier in his career, Johnson was an Assistant United States Attorney for the Southern District of New York (1989-1991).

Johnson is a Fellow in the American College of Trial Lawyers and a member of the Council on Foreign Relations. He is a graduate of Morehouse College (1979) and Columbia Law School (1982), and the recipient of nine honorary degrees.

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the U.S. House of Representatives for the 115th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), or contracts or payments originating with a foreign government, received during the current and two previous calendar years either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. This form is intended to assist witnesses appearing before the House Committee on Armed Services in complying with the House rule. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number) will be made publicly available in electronic form not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary.

Witness name: Jeh Charles Johnson*

Capacity in which appearing: (check one)

☒ Individual

☐ Representative

If appearing in a representative capacity, name of the company, association or other entity being represented: _____

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, please provide the following information:

2018

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

2017

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

2016

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

Foreign Government Contract or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or payments originating from a foreign government, please provide the following information:

2018

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment

2017

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment

2016

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment

*In the interest of full disclosure, though I am testifying in an individual capacity, I am currently a partner in the law firm Paul, Weiss, Rifkind, Wharton & Garrison LLP, and a director of Lockheed Martin and the Center for a New American Security. From December 2013 to January 2017 I was U.S. Secretary of Homeland Security.

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

APRIL 11, 2018

QUESTIONS SUBMITTED BY MS. ROSEN

Ms. ROSEN. As we form public-private partnerships between DOD and industry, I'm worried about protecting the integrity of systems and the integrity of user data. As DOD moves to the cloud, what are the implications regarding public-private partnerships? How do we ensure that we have parallels and redundancies to protect systems and users? Who owns the proprietary information? If not the U.S. Government, how do we ensure that the owner will do their due diligence in safeguarding systems and user information? What happens to data when businesses close or technology is replaced? Is data destroyed when it's no longer used?

Mr. CHERTOFF. The vast majority of the DOD's work with industry comes in the form of traditional procurements, which are subject to a myriad of information security requirements that dictate how government data is secured, handled, processed, retained, and managed within systems provided by industry partners. These requirements are included in all DOD contracts and procurements and are also included in programs such as FedRAMP, which is designed to streamline certification of commercial offerings for use in Federal IT environments. All of DOD's baseline requirements are managed by the Defense Information Systems Agency (DISA) and some procurements may have additional requirements dictated by the individual service, command, or component within DOD. Under these agreements, all government data remains the property of the U.S. government and is subject to the handling requirements set forth by DOD. This includes data retention and destruction policies, which providers are contractually obligated to comply with. These requirements may vary widely depending on the needs of the particular component, the type of data, and the level of sensitivity. It is the responsibility of DOD to ensure that its vendors meet these requirements through code reviews, audits, and other means of oversight. Failure to comply with these requirements can result in civil and criminal penalties for both the vendor and its representatives. At present, all these requirements also apply to vendors offering cloud services to DOD, though there are efforts underway to streamline some of these requirements and adapt them to the realities of cloud environments, which are free of many of the constraints of traditional IT infrastructure. The largest ongoing DOD Cloud procurement, the Joint Enterprise Defense Infrastructure Contract (JEDI), is subject to these requirements, though DOD has pledged to work with the eventual awardee to identify erroneous requirements to speed and streamline adoption. In my view, this is the correct course of action—Cloud environments offer new approaches to security that can enhance data security while allowing for a more flexible and efficient infrastructure. These approaches, such as attribute-based security controls, are promising ways to enhance security and efficiency within its IT enterprise. DOD Cloud contracts also require some level of redundancy for cloud services, generally expressed with uptime requirements (99.99999%, for example) and/or requirements regarding the number and location of data centers, remote storage sites, and hybrid-cloud technologies that can help to ensure the underlying system remains available. That said many large Cloud providers have experienced at least partial outages within their private-sector cloud environments, emphasizing the need for redundancy and resilience in any cloud offering that might underpin DOD operations. To that end, many companies in the private sector utilize what is referred to as a "multi-cloud" environment, which leverages the cloud services of multiple vendors to help ensure that the company's cloud-based IT enterprise remains available even when a single cloud vendor experiences an outage. I think it also worth noting that most major cloud vendors offer government-specific clouds separate from their private sector clouds. These environments are built on separate infrastructure designed to ensure that sensitive government data is not comingled with data from the private sector. In fact, several cloud providers have built cloud computing offerings specific to various levels of classified environments for DOD and the Intelligence Community and include additional safeguards and protections as required by those organizations for the storage and handling of classified information. Beyond traditional procurements, DOD utilizes pilot programs, research agreements, and specialized programs such as Defense Innovation Unit Experimental (DIUx) to work with technology start-ups, labs, academic institutions, and even established technology pro-

viders to identify and develop technologies that meet the unique needs of DOD and its components. Agreements with these entities can sometimes resemble traditional procurements, subjecting the partner to many of the same IT security requirements. In instances where the intent is for the partner to demonstrate and develop a particular technology these requirements are generally less stringent, intended to allow the partner to first build-out and prove a technology before it is incorporated into the broader DOD environment and thus become subject to the department's stringent requirements. In such a development environment the data being leveraged is non-production data, that is, data that is either scrubbed clean of any sensitive or identifying information or a dummy dataset that resembles an actual dataset but is created artificially for development purposes.

Ms. ROSEN. As we form public-private partnerships between DOD and industry, I'm worried about protecting the integrity of systems and the integrity of user data. As DOD moves to the cloud, what are the implications regarding public-private partnerships? How do we ensure that we have parallels and redundancies to protect systems and users? Who owns the proprietary information? If not the U.S. Government, how do we ensure that the owner will do their due diligence in safeguarding systems and user information? What happens to data when businesses close or technology is replaced? Is data destroyed when it's no longer used?

General ALEXANDER. The questions you raise about the cloud and relevant public-private partnerships are important ones. I am a strong believer in the notion that cloud-based systems are inherently more secure and more survivable than classic on-premises systems. At the same time, it is critically important that in implementing the move to the cloud, the government puts in place provisions, in partnership with key cloud providers, for ensuring redundancy of systems and the backup and availability of data, particularly for mission-critical systems. Similarly, the government can and should expect cloud providers to provide assurances regarding the safeguarding of systems, user information, and critical data; it should also make clear—in contractually binding language—what it expects to be done when data is no longer being used, when business closed or are acquired, or when domestic firms come under significant foreign influence. If the government is the buyer, it has every right to set clear and fair conditions on what it buys. These conditions should be vendor- and technology-neutral, but, if put in place should leverage the carrot of Congress's purchasing power. Either along or accompanied by Congress's provision of economic incentives to encourage the development of government-level security, such conditions can incentivize the creation of a more robust cybersecurity environment generally. As a large economic actor—and a key buyer of cybersecurity goods and services—the government has outsized influence on vendors, influence that can reasonably be used to achieve such larger goals of creating a more cybersecure environment for government and industry alike. A good example of this recently was CIA's work with Amazon to create the secure C2S cloud environment. The outgrowths of this capability are making public and private systems with highly sensitive data more secure and resilient. Likewise, the government can and should work with a broad array of vendors in order to find the most capable players in this area and to align these capabilities with government needs on a going-forward basis. Pivoting to cloud makes good sense from a security and resilience perspective and the government should not step back from this effort simply because of issues that can and should be reasonably addressed by industry as part of the government purchasing process.

Ms. ROSEN. As we form public-private partnerships between DOD and industry, I'm worried about protecting the integrity of systems and the integrity of user data. As DOD moves to the cloud, what are the implications regarding public-private partnerships? How do we ensure that we have parallels and redundancies to protect systems and users? Who owns the proprietary information? If not the U.S. Government, how do we ensure that the owner will do their due diligence in safeguarding systems and user information? What happens to data when businesses close or technology is replaced? Is data destroyed when it's no longer used?

Mr. JOHNSON. The following response is on my own behalf, and not on behalf of my law firm or any of its clients. To formulate this response, I consulted cybersecurity experts I know and trust. As the QFR notes, DOD has determined to move toward a public cloud-based solution for the storage of its data, classified and unclassified. DOD recognizes that its thousands of current networks and data centers is not a best practice, and is disadvantageous for DOD and the taxpayers. I appreciate DOD's cautious two-phase approach to the issue, beginning with a tailored acquisition process. To be sure, there are both risks and opportunities for DOD associated with moving toward a public cloud. However, the risks can be minimized and opportunities maximized through the careful negotiation of a contract with the cloud pro-

vider, and such a contract should be designed to address many of the concerns reflected in the QFR. Contract provisions should include at least the following:

(1) enhancement of the cloud's security capabilities and the sharing of classified threat information with the appropriate personnel of the cloud provider; (2) appropriate protocols for incident notification to DOD and response; (3) the ability of DOD to directly detect and address any malicious activity around its stored data in the cloud; (4) appropriate redundancies to protect data systems and users; (5) an acknowledgement that DOD data remains the property of DOD; (6) a provision to protect DOD data and interests in the event the cloud provider closes or is replaced; and (7) adherence by the cloud provider to U.S. government and DOD standards for the retention and destruction of data.