THE BROOKINGS INSTITUTION

FALK AUDITORIUM

THE GROWING THREAT FROM CYBER WEAPONS AND WHAT THE UNITED STATES NEEDS TO DO TO PREPARE

Washington, D.C.

Tuesday, June 6, 2017

PARTICIPANTS:

Featured Speaker:

JAMES N. MILLER
Senior Fellow
Johns Hopkins University Applied Physics Laboratory

Panel Discussion:

Moderator:

MICHAEL O'HANLON
Senior Fellow and Co-Director, Center on 21st Century Security and Intelligence
The Brookings Institution

Panelists:

SAM JONES
Business Development Engineer
Palantir

WILLIAM LEIGHER
Government Cyber Solutions
Raytheon

ANIL RAMCHARAN
Cyber Security Architect and IT Risk Manager
Deloitte

* * * * *

P R O C E E D I N G S

MR. O'HANLON: Good morning, everyone, and welcome to Brookings. I'm Mike O'Hanlon. I won't be up here alone for long, I hope. But I am going to start.

As Jim Miller makes his way past the fourth accident he's witnessed, and I guess maybe that could be a little metaphor for the problems we're discussing today because the kind of dependence on infrastructure that we have in the United States and that could be disrupted are far worse than just four accidents on a regular commute is one of the issues that's before us and before the jury today.

So what I thought we would do, since you've already been very patient and we only have until 11:30, I'll just start with the introductions right now, and then when Jim arrives we'll just launch in. And I'm going to talk first about him and then about the three panelists, who I was going to introduce later but I think I'll just go ahead and tell you a little bit about them now as well so we don't lose time.

And let me first talk about Jim Miller, who was undersecretary of defense for policy until three years ago and had been deputy undersecretary for policy before that. He has now been part of the Defense Science Board and co-authored a study that I think many of you are familiar with on cyber deterrence, but it also talks more generally about other issues with cyber, including the resilience of many Department of Defense systems to various kinds of hypothetical cyberattack and more generally, the resilience, or lack thereof, of the country's infrastructure to cyberattacks. And especially the part of the country's infrastructure that could be relevant to the deployment and operation of military forces because it's not as if we have a clean bifurcation, of course, between defense systems and civilian systems. For example, if we're going to deploy a lot of forces abroad, we're going to use our rail lines and our ports and our airfields to send those forces abroad. Many of those parts of our infrastructure are operated through civilian grids, and therefore, disruptions to those grids could easily affect our military deployments. But the Defense Science Board looks specifically as well at Department of Defense systems. And I thought it was somewhat disturbing and alarming. I'm not going to say alarmist because I think they might have been right, but alarming in terms of the vulnerabilities that many of these systems have today.

So as Jim arrives in a couple minutes, what I want to do is talk through those issues with him, try to establish a little bit of a summary of what the Defense Science Board study this year put forth on the table, how it diagnosed the severity of the problem that we're looking at, what needs to be done

about it, how quickly we can fix these flaws and vulnerabilities if, indeed, they're fixable at all. And then, you know, realistically speaking, how do we handle our vulnerability in the meantime? That's sort of the gist of where I'm looking to go with him in just a minute.

After that, and about halfway through today's system, we will bring up three distinguished cyber experts who will each comment on what they've heard specifically from Jim and about the Defense Science Board study, but also their broader views on cyber. And they're each going to take five or six minutes to do that. We have Sam Jones, William Leigher, and Anil Ramcharan.

Sam Jones works for Palantir and works on cyber issues and has a degree in electrical engineering and computer science from Cornell University and has some experience also inside the Air Force in his previous job. And so we're delighted to have Sam with us today.

A retired admiral, William Leigher, was a Navy flag officer for a number of years including on many cyber command jobs or cyber responsibilities and now addresses these things from a DOD perspective but through Raytheon.

And then finally, Anil Ramcharan works with Deloitte and also has a background and a degree in electrical engineering and cybersecurity specifically from the Stevens Institute of Technology in his case and works quite a bit today with the Navy, but other parts of the government as well.

So I could drag out introductions, and perhaps I should, since that was where I was hoping Jim would arrive in the course of that. And I think we may have to pull an audible here in just a minute in terms of maybe even bringing up the panel right up front.

So since we have folks here, why don't we do that, if you don't mind, because we don't want to waste your time? If everybody can join me. I still expect that Jim's going to walk in at any moment, but if folks are willing to come on up, please. And then to the extent we don't see a quick arrival from our former undersecretary friend, we're going to launch in with a framing of the discussion with these three.

Thank you, gentlemen, for your flexibility.

I think what I'm going to do is ask each person just to give a one more two-minute definition of the biggest problem that they see in the cyber realm today in the Department of Defense, if that's okay. So don't feel the need to solve the problem for us yet. Don't feel the need to give a broad

primmer. And I expect that Jim will walk in in the course of this. But if you could, from your vantage point, and we'll just go down the row, how would you define the biggest problem in cyber today for the United States, but specifically for the Department of Defense?

And Admiral, thank you, and over to you.

MR. LEIGHER: Okay. So quite an audible.

MR. O'HANLON: Yes.

MR. LEIGHER: I think, and you just need to go back a couple of weeks to the Ransomware thing, is we need to do more to engineer kind of the human piece out of the cybersecurity problem. When you had an exploit that was driven by fishing, which all of our cybersecurity experts would agree is the biggest problem -- it's the human user doing that -- we're not doing enough to take actions away from users that prevent cybersecurity breaches. That was a flaw in the Microsoft operating system that had been known for months, yet it hadn't been patched, and exacerbated by the problem of users. We have to be able to do better at the engineering and design level for cybersecurity.

MR. O'HANLON: Excellent.

Sam, over to you.

MR. JONES: Yeah. So it's something that I've been thinking about a lot recently, especially within the context of DOD is how do you turn operators and users on some of the largest networks in the world from a liability to an asset? So specifically in DOD there's a lot of different recording or compliance requirements that are some of the most time-consuming tasks that different cyber operators, cyber analysts have to do on the network. And so what you have as a result is people kind of munging different reports in Excel or, you know, PowerPoint that don't really end up getting used. They spend all their time doing that instead of actually fixing the problem. So we kind of have this, you know, chicken and the egg thing where we either need to get rid of the compliance reports or use technology to actually automate those so that people can be freed up to actually patch these vulnerabilities, fix the network, because right now people don't have the time.

MR. RAMCHARAN: So adding on to comments, for me I think some of the key concerns I run into quite often is just that critical defense capabilities and critical infrastructure were never designed or intended to operate in a cyber-contested environment. I could look at technology today and -- we were

talking about Alexa in the breakroom before here and I could ask a question to the universe about what weather it is or what time it is and I get an answer. It's incredibly connected to the Cloud. That's commercial technology. But our critical infrastructure and national security systems haven't met that level of technical maturity. And if I look at in the cybersecurity space where our adversaries are, they're on the cutting end of technology. They are the most savvy technology experts, the greatest technologists that we have globally operating and trying to defend aging, decades-old technology. So the question to me is not just the skill of the operator but how well we're positioned to actually defend these systems and the structure and the acquisition of those critical infrastructure components.

MR. O'HANLON: Well, thank you, Anil.

And welcome, Jim. And it's great to have you here. So we're looking forward now to our discussion on the nature of the cyber threat today in the United States, but also springing off the Defense Science Board study. I've already introduced you, and although I could have mentioned that Jim now has a number of affiliations in addition to the Defense Science Board, including with Johns Hopkins University Applied Physics Laboratory, and one of the things I really admire most about his career, a lot of us, well, at least myself, I started in the hard sciences and I got soft. Jim was never really a soft guy but he's gotten tougher and more scientific as the years have gone by. And is not only with JHU Applied Physics Lab, but as I mentioned before, a permanent member of the Defense Science Board and a number of other affiliations that really focus on technology and is president now of Adaptive Strategies, which is a consulting firm that does a lot of work around the world on helping other countries build up their defense ministries and so forth.

So Jim, just great to have you here. And what I thought we would do is, you know, spend about a half-hour or so making sure we get some of the basic ideas from the Defense Science Board study on the table and then ask our colleagues to comment. And then ultimately go to the audience, as you know. So of course, feel free at any point to bring up points that I don't get to with my questions, but if you don't mind,

I'm going to begin with a big broad question, which is that I reviewed the DOD cyber strategy reports over the weekend, as well as the Defense Science Board study. I think you were one of the authors of the first one, which was 2011, as I recall. And then there was another in 2015. Those

reports are very good and they're broad because they frame a lot of what DOD has to do in the cyber realm and across many agencies and offensive and defensive and resilient capabilities, and they just struck me as just a very good way to frame the problem.

By contrast, I thought the Defense Science Board study had a slightly more specific focus, and frankly, a little bit more of an alarming focus. As I read that report, I was struck at just how severe the vulnerability seemed to be for Department of Defense systems themselves, because up until then there was sort of a conventional wisdom that I sensed that was developing around town, which doesn't mean it was right, but it seemed fairly common that DOD systems were probably okay but it was more the civilian infrastructure in the United States that was vulnerable. And as I read the Defense Science Board study, I came to the conclusion that maybe everything is vulnerable, and I just wanted to put that question before you and see if that's an accurate reading of the report and its intentions.

MR. MILLER: Sure, Michael. And thanks for that question, for the introduction, and I apologize to you, the panelists, and the group here for being late this morning due to traffic.

If I can step back just a half step, and I'll probably repeat a little bit what my colleagues have already said in talking about our societal vulnerabilities, whether it's the financial sector, the electrical grid, or other aspects of our critical infrastructure, including the part supporting elections as we've seen recently, and that is the Defense Science Board Task Force made a conclusion that the significant vulnerabilities that we have today are going to persist for at least a decade, and they are more likely to get worse over that period of time than to get better.

There is some very interesting technical work going on. Draper Labs has a promising project called Inherently Secure Processor. The Applied Physics Lab where I spend part of my time as you mentioned, has some interesting analogous work and there are others, but even if these projects succeed and are unsubstantiated in the electrical grid and in the financial sector and so forth over a period of time, they will reduce the vulnerabilities and it will be a long-term campaign because there will be countermeasures as well. So that aspect is foundational and a fundamental reason why the task force was asked to look at the questions of cyber deterrence. Yes, cyber defense and resilience are important, but we know that we need to bolster our deterrence posture as well.

And we identified three strategic problems. And if I just go through them quickly and then

I'll leave the prescription discussion for later if you like. But the three strategic problems are, first, the day-to-day problems that we've experienced over recent years of what we call "death by 1,000 hacks." So this includes the 2012-2013 Iranian-distributed denial of service attacks on Wall Street. It includes the North Korea hack of Sony Entertainment for political reasons. It includes the longer term Chinse theft of intellectual property through cyber means, which has apparently gone down rather substantially over the last several years. We can talk about whether that's the case and if so, whether deterrents and other tools are succeeding. And it includes also the Russian hack of the U.S. election. An interesting part of each of these actions is that it's part, in general, of a broader campaign. Cyber may be a domain in a sense unto itself but actions taken there are tended to influence events elsewhere.

So that's problem one. And we can talk about the steps that need to be taken, but they include a long-term deterrence campaign aimed at each of the actors and what we describe as a campaign plan and a playbook, including the use of offensive cyber and other tools, diplomacy and so forth.

Problem two is one that we're seeing just hints of today, but if you subscribe to the prescription of the analysis, I should say the description, of where we are today and where the trends are, it's a problem we could face in the coming years and certainly within the next five to 10 years. And that is to have major strategic vulnerability to lesser actors like North Korea or Iran or terrorist groups and so forth. And from my perspective, the possibility that the United States would be subject to cyberattack that would be debilitating, whether on our financial sector or energy grid to a second-tier actor or a third-tier actor or a terrorist group is an unsustainable strategic position. And that really set the bar for us for what we needed to do for the combination of cyber defense and resilience. And there's a tremendous amount of work to do again in the key sectors -- electricity, water and wastewater, financial, ICT, being certainly at the top of my list.

What it means is that we can't count on deterrence to work against some of these actors. They may be willing to take a chance. Their ability to hold the United States economy and society at risk is such a significant problem that we can't allow it to happen any more than we can with other types of weapons.

And the third strategic problem, Michael, is the largest and the longest term. It's the one

you've alluded to. And it basically arises from the reality that even as our economy and our society have become more and more an Internet of things that our military is already in a very real sense an Internet of things. Each of the services were early adopters of information technology and it's what's in large measure given us such tremendous advantage. And that dependence is not just in the so-called .mil domain of the networks or other classified or unclassified networks. That vulnerability is resident in computer chips embedded in weapons systems and platforms and it's also that vulnerability is embedded in critical infrastructure on which the U.S. military depends for planning for operations for sustainment and logistical support as well.

And the third problem is that the combination of the societal vulnerability and economic vulnerability of the nation with the military vulnerability means that down the road -- I don't see it as the case today, but down the road we could find ourselves in a situation where a major actor, specifically Russia or China, could have the capacity not just to do significant harm to our economy by attacking the electrical grid and financial sector and so forth but could also attempt with some prospect of success to blunt our military response so that we would not have the ability to respond effectively, or they at least may not believe we had that ability and credibility to respond effectively. And that would be a very big strategic problem for the United States. And in short, what we recommended is a very sustained effort over the coming, not just years, but decades on cyber protection, resilience, and diversity associated with (a) nuclear weapon systems; (b) long-range strike that are non-nuclear, because no one wants to walk into the president and say I have some really good news for you, Mr. or Madam President. We've protected our nuclear response capability, and that's all you have. In response to a cyberattack that's an untenable position. So long-range strike as well. And the third category, which is in a sense technically the most challenging, is to have a portion of our offensive cyber capabilities be highly cyber resilient. That has certain implications which people -- I see a number of people who I know are technically expert in the group here who all understand that that's not an easy challenge, but I believe it's a doable challenge. It's not 100 percent guarantee for any given capability but it's an important pursuit as well.

MR. O'HANLON: Fantastic overview.

And let me burrow down on the nuclear forces to begin and then we'll go through a couple of other issues that you mentioned. And I realize there's a sensitivity here because to the extent

we are more vulnerable than people think, there's only so much advantage to be gained by asking a former official to talk about it in public. And I realize there was a classified variance of this report as well. But presumably, you're not arguing in this report that our vulnerability is so stark that it would be straightforward and almost guaranteed and automatic for China or Russia to be able to take down our military forces today.

If I interpret you right, you're basically saying the risk that they could take down parts of these forces is higher than it should be, and they probably can't assess themselves just how vulnerable we would be or how quickly we could recover from any attack they might carry out. So it's not as if they're in a place where they can just risk-free consider a bolt from the blue attack on the United States.

Could you just comment on that a little bit so we make sure we get a clear understanding as much as we can in an unclassified forum?

MR. MILLER: Michael, a very important point. And I expect a number of people in the audience here today have read Ghost Fleet. I thought it was a terrific book. That -- I don't want to -- I guess spoiler alert -- slight spoiler alert. It's a scenario in which there is a bolt from the blue, including cyber and space that take down critical U.S. systems. I think that is by far the least likely scenario. And I think it's made only slightly more likely by the cyber vulnerabilities that we have.

The scenarios that I'm concerned about are in two other categories. One of the escalation of a conventional conflict in which as things get going, each side may have very strong incentives to use cyber tools against the other side, as well as counter space capabilities if they have them and, you know, projecting forward one could imagine that that would be more the case than it is today.

The advantage of using cyber early on in a conflict, in a major power conflict in particular, is that you could hope to delay and degrade the movement of the other side's forces and the employment of those forces. You could attempt to gain coercive advantage early if you can demonstrate that capability by using it. And then the reality is if it succeeds, there are no direct and immediate casualties. There may be over time other causalities. And if it doesn't succeed, the other side may not know you even tried. So it's something that I think on the cyber is going to look very low risk to use early in a conflict, and similarly for outer space where the reality is I don't think either side is going to go to major

conflict because it has a couple of dead robots in outer space, just to be blunt.

So the escalation of a conventional conflict given the incentives to go early in cyberspace and potentially outer space is a concern. And second, whether it arises from back and forth in cyberspace, whether it raises from a war of words in which cyberspace plays an increasing role, I think there are, in a sense, new pathways that come predominately from cyberspace and from the war of words, if you will, that could escalate quickly and that could then involve the posturing of forces. And if I want to gain an advantage, if one side wants to gain an advantage in that even in that war of words and that non-kinetic cyberspace conflict, showing that can have some effects on your weapon system that reduce your credibility internationally to intervene that reduce the confidence of your leaders and so on is likely to be an attractive avenue for each side to take. And it's really because of these stability concerns of escalation that I want to highlight the issues associated with the vulnerability of our military forces. Because just as we've taken steps over the years to put our -- during -- when we had only bombers -- put our bombers -- for nuclear head, put our bombers on alert and so forth to harden our ICPMs to take other -- to put our submarines -- missiles on our submarines underseas, just as we've done that in the nuclear arena, we need to tape steps with respect to the electronic and cyber components associated with nuclear and key conventional systems in order to reduce the incentives for the other side to take action early in a crisis or conflict that could cause escalation. And frankly, I believe we should welcome those types of steps by the other side as well, by Russia or China, in particular, because we don't want them fearful that we would do that to them. And the fundamental challenge here is we had a range of tools in arms control where we got used to counting nuclear delivery vehicles. We never have been able to count nuclear weapons accurately, but nuclear delivery vehicles. And we're able to see the large infrastructure that's associated with the deployment of nuclear systems and large-scale conventional systems that just isn't the case for cyberspace and counter outer space systems.

MR. O'HANLON: So if we -- if we look at the Defense Science Board saying that vulnerabilities are not only severe today, they're going to get worse, and therefore, we have to prioritize our response to make sure that at least within a decade we have our nuclear forces and long-range conventional strike forces reliably available, that implies that, you know, things are pretty bad and getting worse today and it's not even realistic to aspire to protect all the general purpose forces in the first

instance. It's going to take too long, and because the problem is so severe we're going to have to accept that vulnerability for a while if I'm understanding correctly. So could you comment on that? And also, what does that mean exactly? If I imagine an Army brigade, a heavy brigade combat team, it's not going to be presumably one of your top priorities. I mean, you're not saying to ignore vulnerabilities for a decade but you're saying maybe that has to be a somewhat lower priority than the nuclear forces or the long-range bomber force. That brigade over the next year, if it's attacked, what is the likely consequence? Are we likely to see that brigade just get to the point where basically nothing works because even the tanks, even the artillery systems have their own computers today and their own software? So if there are vulnerabilities, you could literally see the entire unit more or less be shut down? Or is it more likely that you're going to have an attacker figure out a vulnerability, let's say in one element of that brigade combat team's capacity? Let's say it's certain tactical radios or, you know, the helicopter fleet's ability to properly use its sensors. In other words, something discreet and serious but not catastrophic to the unit?

MR. MILLER: Michael, that's a great question. Certainly today, and even 10 years from now, I would expect because of the diversity of systems in the general purpose forces, including within services as well as between services, that the prospect of any attack being able to comprehensively take out even a single brigade combat team or even a single win of aircraft or even a single carrier battlegroup is very unlikely. Today, and likely in the future for conventional forces because I would expect them to be less of a priority for potential adversaries than our strategic capabilities that could go against -- more directly against their strategic capabilities, if you will, I think about three scenarios.

One is the insertion of false data that causes the BCT or the other units to act on inaccurate information. And that's something, obviously, that's part of the fog and friction of war and that has to be dealt with. This is an amplifier. The cyber vulnerability is an amplifier to that.

Second is the disruption of communications that causes orders not to be promulgated and so forth. I don't believe it's at all likely today or in the near term that that would be comprehensive. And in this scenario, cyber warfare would be added to the broader electronic warfare of attempting to suppress radio communications and so forth as well.

And then the third category is what you alluded to I think most directly and that is for

some systems there may be, whether through the supply chain or a previous insider access or through something that's done near real-time remotely, there will be vulnerabilities and there may be accesses that would cause them to perform improperly and for missiles to go the wrong direction, for guns not to fire and so on. And I think that we will see some of that in combat, certainly between major powers. If that were to occur any time going forward today there would be some degree of that. And the military has to be prepared to operate in that environment. And I'm very pleased when Marty Dempsey, general and former chairman of the Joint Chiefs, Marty Dempsey and the leadership he put forward and directive that required all exercises essentially to begin to deal with this issue. I think there's work to be done there, and it's important work. But you're right. I view it as less -- I view it as -- although it's a today problem, it's not likely to be the same level of a strategic problem as the vulnerability of nuclear long-range strike and offensive cyber.

MR. O'HANLON: I really just have one last question.

SPEAKER: Can you speak closer to the mic? We can't hear you at all back here. Sorry.

MR. MILLER: Yeah, yes, I can. Thank you.

MR. O'HANLON: Okay, thanks.

So one last question, Dr. Miller, if I could. And I guess it's sort of a two-part question but I think they connect. And one is I'm trying to figure out how we got so vulnerable. And I think I know parts of the answer but I'd love your comment. But then that leads to the next question of how will we know when we fix the problem? In other words, the Defense Science Board talked about a 10-year time horizon for addressing the most important -- again, just to keep drumming home that key point that it's going to take us 10 years even to partially fix this problem, but that implies the problem is even fixable. And I realize there's probably never going to be an era of perfect cyber resilience and impenetrability. But clearly, the implication in the Defense Science Board study and much of what we learned in the cyber realm and probably what some of our panelists work on in the day-to-day lives as well trying to make DOD more resilient, the implication is that there are better practices that we can adopt now and in the future than we've been using in the past because we somehow created these vulnerabilities in the past and there is a path forward to eliminate them. It's going to be slow and costly but it's going to take time. So, my guess is that some of the others will want to comment on this in a moment as well, but how did we

get so vulnerable? And then how do we make sure we really can fix this thing? What do we do differently in the future to make sure we don't just recreate new vulnerabilities that are exploitable themselves?

MR. MILLER: So we got significantly vulnerable because we took advantage of the information revolution with our military. And Michael, you will remember -- I'm dating us both a little bit -- in the late '70s and through the '80s, a big debate about whether the combination of information technology, precision strike and advanced intelligence, surveillance, and reconnaissance was going to have a big impact, what the Soviet Union at the time was calling the military technical revolution. That was proved out initially in Desert Storm and we had seen elements of it before but the military very intelligently pursued this important strategic advantage that allowed the military to perform to extraordinary technical levels in recent conflicts. You know, that technology, married with the incredible people that we have in uniform, not just their capabilities as they come in but their education, training, and ability to operate in a disperse mode and make decisions at a much lower level than most other militaries has been a fundamental advantage to us.

So the technology was there and it gave us tremendous strategic advantage. We've been, as a nation and as a military, we have been slower than I certainly would have liked to address these vulnerabilities and it's clear that there is substantially tension at the national level today on the vulnerabilities of our critical infrastructure. And I think that's important. I was frankly disappointed not to see more progress of legislation over recent years on that score.

But going forward what it means is that we need to do in broad buckets three things. So first is prioritize. And the Defense Science Board Task Force on Cyber Deterrence put forward what we thought should be the priorities. Again, high defense and resilience for nuclear strike, a substantial capability for long-range, non-nuclear strike. Not the entire force but substantial. And then offensive cyber. And that will be a very significant investment and that will be challenging to accomplish, and we won't be able to prove that it's complete or successful, but what we will be able to do is through a combination of advanced technology, applying new technologies, and applying both smart diversity of systems. So if you get me in one place you won't be able to use the same trick to get me in another place. And then smart changeover time so that you don't have the ability to study the same operating

system or can count on the same combination of chips being put together for a mission, if you will. Those will be important as well. And one of the recommendations was to establish a program of best practices in that regard. So prioritize and invest -- it will be a substantial investment.

Second, keep working hard on the critical infrastructure of the United States because at the end of the day we must get that threshold -- or sustain a threshold where terrorist groups and lesser powers -- the North Koreas and Irans of the world -- do not have the capability to hold our nation at risk through cyber any more than they do through nuclear weapons or any other tools. And that is going to be a major effort on that front.

And the third thing that we need to do and that we can -- I'm sure everyone else will have views on this as well, I believe we need to have a policy of responding to cyberattack. It doesn't mean to every intrusion or every attempt, a cyberattack, but in any instance where we judge there's a significant cyber intrusion or cyberattack, the questions should not be whether to respond but how to respond. And we need to begin to demonstrate that on a systematic basis at least going forward.

MR. O'HANLON: Excellent. Well, thank you very much, Jim.

And now we'll move down the panel speaker by speaker, starting with the admiral. And you know, I really would just ask that you comment on whatever you think needs to be added to the discussion at this juncture. Any points of either reinforcement or disagreement or nuance in regard to Jim and the Defense Science Board study. And if you need anything beyond that, I'm sort of now intrigued by the question at what point is the United States going to be at its moment of maximum cyber vulnerability? It sounds like the Defense Science Board thinks things are still getting worse every year, and the question is how fast can we arrest that so that maybe 2018 or 2020 would wind up in retrospect being seen as the year of maximum vulnerability? Maybe that's an optimistic assessment, I don't know, but if you need anything else to react to there's one more question.

But Admiral, over to you.

MR. LEIGHER: Jim, thanks very much. And I would congratulate you and your team at Defense Science Board for a really thought-provoking report. It is taking the discussion about cyber in the direction that it needed to move in.

I would say most of what I would comment on is nuance. And first it comes back, along

with the issue of DOD bought into the information age pretty quickly. We only did that with those people who branded themselves as IT professionals, now cyber professionals. And when I talk with the engineers who aren't the cyber engineers -- so aeronautical engineers, naval architects, people who are designing the system, they've always done a great job in what we would have said, you know, in a Navy discussion, designing (inaudible). Reliability, maintainability and those things. But those same engineers have given almost no thought that there's a hacker out there who's trying to break their software. And that's really the key of this. This is what cyberwarfare is really about. It's about breaking software and finding that vulnerability. It's a targeting problem that's not really unlike any other kinetic targeting problem. It's just a different discipline approaching that.

And I guess I would take a little bit of disagreement in thinking about the vulnerability at the unit level. If you can stop the generators on a DDG-51, it's a non-mission capable platform, it can't defend itself. It has no ability to project power. And I think that's an easy one for me to get to with my Navy background, but I think you could go to an Air Force officer or an Army officer and find similar analogies where the weakness really is that stark. And again, it's the same issue at the operator level where you'll find tactical action officers and operations officers across the force really thinking about their vulnerabilities but they don't think about the vulnerabilities and what it's going to take to recover from that kind of cyberattack.

The second thought is the international piece. And this is something that I worried about, you know, I would say since Terminal Fury 10 when I understood how difficult it is to interact with our key allies when it comes to sharing cyber threat warning information. And I think it's only been exacerbated by then. Since then, I think there are some things with basic sharing of virus signatures and things like that's improved, but at the same time we've opened up to our allies, you know, more pathways to systems like Link 16 Joint Strike Fighter international sales. It's something that ought to concern us from a cyber perspective. Every time that we have an FMS case that bolsters certainly the Pentagon's budget and the ability to get some economies of scale with platforms we're also incurring cyber risk and we really haven't accounted for that in how we think about our alliances.

And lastly, you know, with the executive order that was released a couple of weeks ago, I think we also need to think about this problem in a whole government perspective. I know the Defense

Science Board is chartered by the Department of Defense, but the EO didn't really have a roles and missions change at all. It suggested that we're on the right course, but the truth is DOD has very little responsibility for our banking. DOD has very little responsibility for our power grid. And it was always my key worry at Fleet Cyber Command that my sailors, because DOD has the capacity, were going to be the ones who ended up responding to attack someplace across the critical infrastructure sectors and they weren't trained to do that.

So I do think there needs to be some examination of roles and missions. That includes a couple of things. General Hayden is the first guy I heard talk about this, but industry owns the Internet. We can think about that in a lot of different ways, but our bit bandwidth providers really have a key stake in this that probably goes beyond anything that we can think about. And then when you get back to the fundamental defensive problem, I don't think we've engaged the military industrial complex well enough to help solve this cyber problem on the defensive side and give us new deterrent solutions.

MR. O'HANLON: Excellent. I'm going to actually follow up with one quick question to you, Admiral, before we go to Sam and then Anil, because, of course, we're at a period of flux in the command arrangements now with the U.S. military on cyber, right, and we now have the ongoing gradual creation of an independent cyber command but it's sort of not yet fully born if I understand things correctly because we still have the same director of the NSA and cyber and we also haven't fully populated a new command.

So could you just very briefly describe, you know, who is responsible for what today? What are the service's responsibilities for their own equipment and fixing their own problems in their own software? What's the responsibility of the unified cyber command? And to what extent does unified cyber command even yet exist?

MR. LEIGHER: We don't have time enough. So, you know, I think in general, Admiral Rogers is responsible for the defense of the DODN and for supporting COCOMs and projecting power through cyberspace. The problem is we don't have a lot of experience in any of that in terms of how it goes. When you get to this issue of the OT side of it, I think there's a lot of confusion with who really owns the problem. I've heard two service cyber commanders basically say this is not their problem. Their problem is the fundamental network and defending that. I think we've got to sort that out. When

you get up to the next level, certainly, cyber command because for the same reason the dual (inaudible) happened in 2009, the majority of our intellectual capital still resides at Fort Meade and around that. So I don't think Admiral Rogers will be able to, you know, escape having a lead role in that. But when you go the other way, I think you've got to look at what DHS's role is, and is DHS strong enough to really provide the leadership and the technical capacity to respond when it comes to the critical infrastructure piece which by our policy they're primarily responsible for.

MR. O'HANLON: Thank you.

Sam, over to you.

MR. JONES: Great. Thanks, Jim. Thanks, Admiral, for kicking off a great discussion.

I think I'll spend most of my time commenting on how do we actually secure ourselves in the near term and long term taking kind of a data perspective from it? So I split it up in short term and long term because I think we already have been focusing the discussion on that as what can we do in the next five, 10 years, and then what do we do 10 years out planning to be more resilient?

So in the short term, I think we have to get a lot more creative. And so what I want, you know, the DOD especially to be able to do in the short term is to be able to holistically look at risk, both from an enterprise network and non-enterprise network. So this would be mission systems that we've been talking a lot about. And actually prioritize this is where I'm going to spend my time. Because we don't have enough time to fix everything, to modernize everything, but we should be in a position where we can actually look at what the data is saying and then make the best use of our time to actually fix the problems. So I think we can all agree, you know, nuclear systems should warrant more attention then, you know, a legacy HR system. But, you know, the problem doesn't get so clear cut when you start looking at things in the middle.

So getting creative with enterprise systems. You know, DOD is operating some of the largest networks in the world. Probably DODN by itself is the largest network in the world. And it wasn't built to be instrumented in real time and to be defended in real time. However, there are data systems and data sources on that network that will allow for, you know, operators to get, you know, maybe 80 percent view into the network in real time. But some of those systems that, you know, I would look at instrumenting for that purpose weren't actually built for that or not actually thought about that. So you

have to get creative in that sense.

And we've been talking a lot about, you know, mission systems, but the enterprise systems, the enterprise network is also vulnerable. And while it's not, you know, maybe not as critical as the nuclear systems, that HR system might be highly vulnerable and it could be susceptible to be going down, you know, any moment.

Now, for mission systems, you probably need to get even more creative at this point when we're talking about, you know, whether it's tanks, something on the grid, plane, ship, whatever, there's embedded processors there. There's a lot of different electric components that -- there are ways to instrument it and get a sense of, you know, what's actually on board? What's the state? How is it configured? How can I now have, you know, maybe a static snapshot of what may exist and then prioritize from there. And kind of these two things together, kind of the enterprise systems and the mission systems, the final kind of component from a data perspective the way I look at it is you have to assign or kind of map out what is this thing functionally doing? What is it responsible for? Because a lot of times, especially in kind of the legacy IT systems, it might actually be supporting a really important mission. It might be supporting a really important unit. But there's nothing that actually says that this server is supporting that.

And so it's not going to be, you know, this is where a lot -- I've seen some different papers about, you know, we'll deploy this either like neural network or you know, some different algorithms to map our network for us, but it's not going to be a glorious process to be able to, you know, extract operator knowledge and layer it on top of some of these other systems, other data sources that describe out network, but really, this knowledge needs to be extracted so that commanders at the DOD level have the ability to look at, you know, these are the missions that I really care about right now. Here are the different systems, both enterprise and mission systems that are supporting that. And here's where I'm going to spend my time in the next, you know, one month, and then one year, et cetera.

Now, that's kind of how I view the short term. Obviously, longer term, I think the DOD needs to get really aggressive about modernizing. There's already lots of efforts about, you know, removing legacy IT systems, things like that, but I would, you know, I would fight for an even more aggressive approach. You know, if there's legacy, you know, databases, systems on a network, they

should probably be removed. And if anyone is suggesting that you should build something, you know, on premise, you need a really good argument of why you can't do that in the Cloud. Because we've talked a lot about all the different systems on the network right now were not built necessarily with security in mind, but if you go deploy a new application in AWS, a lot of those services are built for security in mind. They're rebooting every single day. They're instrumented very, very well. You can patch things immediately. And so we're going to have to get a lot more aggressive about moving ourselves over to that type of infrastructure, which is going to be a very difficult challenge. But I think it's one that we need to be extremely aggressive about so that in 10 years from now, you know, our enterprise legacy, IT footprint looks a lot different than it does today.

MR. O'HANLON: So just one clarifying question with you as well. So just to sort of beat the point home and make sure I'm hearing it in the simplest English possible from a generalist point of view, you're saying that there is a way to write much more resilient, much better code than what we've typically done in the past. It may not be perfect, and getting to Jim's point, it's important not to develop codependency across all different systems in case you, nonetheless, have a vulnerability in your better code that you didn't want or anticipate, but generally speaking, you can lower the risks of having vulnerabilities in your code by orders of magnitude if you write it correctly. Is that essentially what you're saying?

MR. JONES: Yeah, absolutely. And part of it is using the right software, the right systems, but a lot of it is also internally having the right, you know, ABSEC, you know, teams that have aggressive policies. But it probably is something that at least, you know, I came through, you know, the college system not too long ago, is the security component of, you know, the computer science course that I studied was almost not there. And so a lot of the people that are actually going out and writing code now have little to no software experience. So that would definitely have to change if we're going to make a meaningful effort so that, you know, it's not just you're either a security search or a software developer. You're always both.

MR. O'HANLON: I'm going to actually give both of you the floor here one more time and then we'll get to Anil, but I want to ask Sam a question and let Jim respond, too, or whatever else is on your mind, Jim, please bring it up.

Sam, can you give me -- I realize we're not going to get into a course on or a lesson on writing code here at Brookings today, but can you give me like even a little bit of a feel for what you mean by writing code with security more in mind? What does that actually mean in terms of improving vulnerability?

MR. JONES: Sure. So you know, a common example of how you might attack a website is something called like cross-site scripting. It's like a really common thing that a lot of people don't even realize or learn about until they might actually go develop something and then, you know, several iterations down the line someone's yelling at them for their code being vulnerable because it got scanned for the first time or something like that. It probably just means, you know, having good teams that are constantly reviewing themselves and maybe having an internal expert on your team that's always assessing their code and can engage at the right technical level to, you know, actually understand how everything is working, and then having the right application security teams that are kind of red teaming everything that you're doing from the start as opposed to, you know, we just released our beta version of an application and it's now live; let's now think about security. It should always be at the start of the discussion, and essentially, you just need to be kind of fluent on kind of the top different types of threats and then design for those from the start.

MR. O'HANLON: Thanks.

Jim?

MR. MILLER: Just two quick comments and I think it's valuable, Sam, that you raised the question of enterprise systems because elements of the first date of the operations of the Department of Defense and others will ride on those, and second, in crisis or conflict there will be important ways used as well, including, for example, U.S. Transportation Command which relies on the unclassified so-called NIPRNet to communicate with a lot of providers of logical support in transportation and so on.

Just an observation that if you want to make a computer 100 percent secure, don't turn it on. Right? And that's about all you can do. If you're looking at what could a top tier nation state do over a period of time with the range of tools that it may have, including potential recruitment of insiders, including potentially close access as well as the other tools that we think about, including supply chain, I think you've got to realize that you do want to think about security, you do want to reduce those risks as

much as you can, but you've got to think in terms of resilience and redundancy as well. And when you think about red team, you think not just about the pen testing that is done in information technology, but the broader red teaming of the type that's done in our SSBN security program where you have a group emulating an adversary and what would a sustained campaign look like over a period of years. And then develop capabilities to counter those -- not just those known threats but those potential threats that can be most damaging. And I think the Navy has been at the forefront of red teaming nationally in both of those senses.

MR. O'HANLON: Excellent.

Well, Anil, thank you for your patience. You're our cleanup hitter, so your reward for your patience is the bases are now loaded, I think, or whatever metaphor. But don't throw your helmet, but do whatever else you want to do now at this point to complete the conversation and then we'll go to audience questions.

MR. RAMCHARAN: So building on some of the comments around understanding adversarial landscape and escalation in terms of using cyber as a warfare mechanism, what I think is incredibly interesting is tactics and techniques being employed in cyber warfare are incredibly intricate. Looking at an analogy on conventional warfare, geography is not a problem for cyber. Concealment is not a problem for cyber. The barrier of entry is incredibly low. There are tools out there on the Internet that are usable today with a savvy Google search that could really cause significant problems. These aren't major defense acquisition programs that require Ph.D.s and billions of dollars to affect a cyber incident. It's low cost, low entry, sometimes low skillset with the toolsets that are out there.

So when we start to look at capabilities, such as attribution and the appropriate response in terms of deterrents, it enters an interesting space because I think we're seeing some of those traditional norms in conventional warfare not necessarily apply to cyber landscape. I can create as much impact on economic, political, and social stability as hacking as commercial institution, or a healthcare institution, or a public works utility institution, as much as I can defense national security capabilities. I think that ends up in an interesting policy landscape in terms of -- I know scope being Defense Science Board, but how does that support national security as a whole and what does that public-private partnership look like in terms of cybersecurity?

MR. O'HANLON: So implicitly, are you saying that while you certainly share the concerns that you're hearing across the board about our DOD systems, that you think the civilian infrastructure is likely to remain far and away the more vulnerable or is that reaching too far from what you just said?

MR. RAMCHARAN: I think the target landscape is broadened. And when we used to think of warfare as being military against military against nation state adversaries, I don't think that's going to apply. I think if you track some of the major cyber incidents -- I think we've mentioned Sony, we can trace that to nation state adversaries, but through a proxy. Through intermediaries that are affecting those cyber effects. Well, that's now a really interesting place because it's possibly attributable to a nation state adversary but activist groups, malicious crime organizations, other entities, named Anonymous, for example, that are out there creating these cyber (inaudible), sometimes at the behest of nation state adversaries, sometimes on their own. So when we start to look at deterrents as a capability and what the appropriate response to that is, I think the part that does apply for kinetic warfare is how do you make the right attribution? How do you measure the response? In the cyber environment that's incredibly difficult.

MR. O'HANLON: Let me stay on -- you mentioned attribution -- let me just stay on that for a moment. Again, asking one more minute of delay before we get to your questions. But attribution is a delicate thing to talk about in an unclassified domain as well, but -- thank you for raising it anyway, and I'm of the opinion or of the impression that we're actually a little better at it than we sometimes led on. There are good reasons not to get too specific so I'm not asking any of you to go too far in this realm. But I'd like to begin with Anil and others may want to -- what's the likelihood -- it seems like we generally can figure out who is behind something. We may not be able to prove it in a court of law but we can prove it to our own satisfaction. And therefore, that may or may not be adequate in a given case for public shaming or what have you, but it's usually adequate for us doing something in rely it would seem. But maybe if you're trying to use international sanctions, for example, you've got a hard time building your case if you're not trying to give away sources and methods. Can you just talk a little bit about how good we are at attribution and how much better we have to get?

MR. RAMCHARAN: Sure. So I think things that are human nature, we're creatures of

habit. We have patterns of behavior. We have known motivators that if we were able to profile geopolitical landscape and you're able to help get a sense of who your adversary is and how they would act and respond in specific situations. And I think cyber is no different. I think when we see different tools of the trade or techniques being employed in cyber effects, we can trace the lineage of who uses those kinds of methods to help us better understand what that landscape looks like, which then leads us down the real road of intelligence more so than evidence, which is a key aspect for us thinking of national security.

I think above and beyond that, when we're looking to plan response based on that information, that's where we've got to be measured. Whether it's an actual cyber response that we're going to employ, sanctions, whatever the technique may be, because it can be out of band. Cyber effect doesn't necessary mean cyber response. There are other avenues for us to enact those controls. I think that's where -- to make sure that we're operating appropriately, we enter a space of understanding what real evidence we have.

MR. O'HANLON: I'll give the floor quickly to Admiral Leigher and then to Secretary Miller on the same question. Then we'll go to the audience.

MR. LEIGHER: Yeah. I think we need to take a step back and think about where our attributions started, which is fundamentally by using cyber means to collect intelligence. It's an act of espionage. We do not want to be put in a position where it's understood that we're the culprit or any country wants to be in that position. So I think when you get over to the defensive side, attribution isn't necessarily the correct approach. It's do we have the right intelligence requirements and are we tasking the system to appropriately understand who is trying to target our critical infrastructure and what we need to learn from that to bolster our defenses. It's a much more traditional approach that we would use in defense against any weapon system. And again, I think cyber has to take a lesson from that.

MR. MILLER: Two quick comments on this score. First is that we've been implicitly talking about attribution based on technical analysis, whether it's the specific code that's embedded or it's the craft associated with it. And that's an important tool. And second is attribution through intelligence collection, whether signals intelligence or human intelligence. And those two have different thresholds for release of information obviously.

A point here is that if we are able to raise the bar to reduce the vulnerability of our key systems to intrusions by criminals and activists and terrorists and lesser states and so forth, our ability to attribute will be much easier because there's a smaller set to look at of states and actors who have the technical tools required to do this kind of higher skill intrusion and attack.

And finally, the gold standard on attribution -- we think about three attributes. One, we'd like it to be instant. So what's the timeline it takes us to do it? Second, we'd like to have 100 percent confidence. What's our level of confidence based on multiple sources is then a question? And third, we'd like it to be publicly releasable. So if you could have an instant, 100 percent confident, publicly releasable, that would be great. And then as you think about the different elements that you bring into making a case for attribution, different types of information will contribute in different ways to those three different dimensions.

MR. O'HANLON: Excellent.

Okay, please, if anybody has questions, please wait for a microphone after I call on you and identify yourself. And if you want to pose the question to one of the panelists specifically, that's great, or you can make it more general.

Anybody want to kick it off? I'll take two or three at a time. So we've got the gentleman here in the fifth row. And then further back in the tenth row. We'll start with you two.

MR. CARBERRY: Thanks, Sean Carberry with Federal Computer Week.

I want to drill down a little bit more on the deterrence conversation. That's something that's been a huge topic of discussion on the Hill. A lot of senators have been pressing for a deterrence strategy, but a lot of people who, in response to that are saying, look, there's no model that works in cyber. The nuclear model doesn't work. The only thing you can do is deterrence through denial, resilience, those kinds of things. What are some of the things that you've explored what models do or don't work? How do you come up with a deterrence framework? And especially when you're talking about these sort of second and third tier actors who aren't going to play by the same rules as nation states?

MR. O'HANLON: Let's take one more before we get responses. So, perfect. Thanks.

MR. BUCHBINDER: Andrew Buchbinder from PILPG.

Jim, you spoke specifically about systematically responding to significant cyberattacks. Could you speak a little more on what that would look like in your opinion? What you believe should be kind of a uniform approach to that type of attack?

MR. O'HANLON: So Jim, over to you to start and then let others comment as they wish.

MR. MILLER: Sure. Andrew, I would not argue for a uniform approach to respond to cyberattack or serious cyber intrusions. I'd argue for a tailored approach, for it to be tailored to the actor that we are trying to deter. And in order to deter them rather than just respond to them, you need to have a plan in advance. You need to communicate to some degree your capabilities and intent to respond. Some of that is done through action, not just through speeches and so forth. But this is why I do believe strongly we need sort of a campaign plan construct and that campaign plan for cyber deterrence needs to be embedded in a broader deterrence construct with respect to these key actors. And I would specifically include Russia, China, North Korea, and Iran. And it's important to include that forward looking as far as their response actions because each one of those actors has the potential to escalate beyond an initial cyberattack, whether through additional cyber or other actions and we need to think clearly through what that escalation may look like when we're responding and to deter them not just from future cyberattacks of what they've done but deter them from escalating against us or our partners and allies in the context of our response as well.

And for Sean, it's a great question. We've spent many hours debating alternative models. Let me just note three. Criminal justice, conventional deterrence, and nuclear deterrence. In the criminal justice model, there's a sense, an understanding that potential criminals will sense some probability that they're caught and punished, and then there's a severity of that punishment if that occurs. But there's not any expectation that criminal deterrence is going to -- even if it's highly successful, that it will prevent all crime. And I think there's certainly an element of cyber deterrence that's in that genre, whether you're talking about the broader deterrence of criminal activity where it's obviously applicable that analogy, or even with respect to nation states where they're going to be testing the lines of what they can accomplish. And we're going to have to find ways in which to clarify our policy relative to today, and also build case law, if you will. And getting some consistency in that within and across the administrations is going to be important.

If you think about a second analogy of conventional deterrence, which has been fundamental to the U.S. military posture going back, you know, many decades, even with nuclear deterrence laid on top of that with respect to some actors and particularly with respect to the Soviet Union for a period, conventional deterrence has been fundamental to what we are trying to accomplish in Europe and Asia, in the Middle East in particular. And yet we don't think that conventional deterrence is going to prevent all actions by adversaries, and we know in some instances that signaling is very important, whether it's signaling by the movement of forces. For example, flying B-2s and B-52s over Korea over recent years. It's a signal of capability and of assurance to our South Korean allies and Japanese allies as well. So I think there are important lessons on the conversational side.

And on the nuclear side there actually are analogies and lessons. The most important one is that deterring Russia is not the same as deterring China. It's not the same as deterring North Korea. It's not the same as deterring Iran. Even from nuclear employment, let alone in these other areas. And that means you've got to have so-called tailored deterrents, tailored to the potential adversary. Tailored to the circumstance. You need to think it through in advance. You need to not make huge assumptions about what you know and don't know given that when the Soviet Union collapsed, for example, we found that the United States had fundamentally misunderstood their thresholds for nuclear escalation and needed a strategy that's robust to error. Those are important lessons, as well as from nuclear deterrents.

And one thing we shouldn't take from that, people who have spent their careers in nuclear deterrence tend to think defenses are irrelevant, whether it's passive defense, civil defense, or whether it's missile defense, they're irrelevant with respect to a large actor like Russia. In particular, Russia. In cyber deterrence, that's just not the case. Defenses and resilience are the fundamental starting point for an effective deterrence posture, both to raise the bar for even the most capable actors and to crowd out others and for the credibility associated with any response.

And I'll finish with this thought. By analogy, if I were leaving boxes of $100 bills out on my front porch -- I don't have them, so don't bother Googling where I live -- but if I was leaving boxes of $100 bills out on my front porch every night and they were disappearing every night, the reality is that, yes, someone would be breaking the law and that person or persons should be brought to justice. No

doubt about it. But at the same time, if that happened and I walk out and put beside the piles of money I put explosives, I'm liable to go to jail as well. Taking due diligence to protect our own information systems in other words is fundamental to the credibility, both from a legal perspective and a domestic and international political perspective to be able to take strong responses when somebody doesn't just take the money off our porch but breaks into our house and breaks into our safe to take that.

MR. O'HANLON: Thank you. Any other thoughts on those questions? Anybody?

Okay. We'll go to another round of questions. Good, we've got a couple in the back. Let's take -- actually, all three I see in the very back together. So I see one person standing, one person sitting in the back row, and a woman sitting in the next to back row. We'll take all three of those, please.

MS. GREENHALGH: Hi, I'm Susan Greenhalgh from the Verified Voting Foundation, and I have a two-part question.

The first is, there are reports that the Russian government has taken the step to take all classified information off of any type of computerized equipment and put it back on paper from a typewriter and transfer it physically from one place to another when it needs to be done. I'm not sure if that's correct but that's been reported. Do you see any future for us to go and take parts of our infrastructure entirely offline and back to some sort of process like that?

And separately, right now we know -- we heard the story that came out in the Intercept yesterday about the NSA report and the Russians targeting actual parts of our election infrastructure. What many people may not know is that currently, 32 states permit military and overseas voters to return their ballots over the Internet to vote online. And that's a process which is obviously quite insecure. These are military men and women protecting our democracy. I wonder if you could comment on that practice.

MR. WATERMAN: Yes, hello, Shaun Waterman. I'm a reporter.

Jim, I wonder if you could drill down a little bit more on the question of the trend line on this. I mean, was Mr. O'Hanlon's characterization of the board's report that things are actually getting worse at the moment, that we're approaching the point of our greatest vulnerability rather than watching it recede in the rearview mirror? And why is that?

SPEAKER: Hi, (inaudible) Times. I've got a follow-up question for James regarding the

answer to the first question. You mentioned about there needs to be a campaign to demonstrate our deterrence capabilities. But what specific idea do you have? How do we go about demonstrating those? Because I think that right now what's needed is not only to demonstrate capability but allowing us to hit back at whoever is hitting us, like the actors that you mentioned, Russia and China. I think they understand perfectly we have that capability. But I think that the (inaudible) show that we have the willingness to use those when the time comes.

MR. MILLER: Okay. I'll go in reverse order if that's okay.

To demonstrate capabilities, fundamentally there are three approaches. One is to release information about them, which is effectively what we've done with our nuclear weapons, if you will. The demonstration on August 6th and August 9th at Hiroshima Nagasaki was for a different purpose, not for demonstration. So it's information. It's then to, second, to apply those capabilities in an exercise and so forth, and the third as you suggest is to use some of those capabilities in the real world against real world adversaries in response to their actions.

Let me make clear that as you think about both a campaign plan and sort of a playbook to bolster our deterrence posture and to respond to intrusions, it needs, as Admiral said, it needs to be a whole of government approach. And the first tools that you pick off of that shelf are going to be diplomacy and economic sanctions and political steps to reinforce our alliances and partnerships and so on. But without question, offensive cyber capabilities need to be part of that mix because any actions can escalate. We need to think that through. But since I raised escalation before I'll conclude this answer with this thought. If we take action, there's a risk of escalation. If we never take action, there's a certainty that we'll face escalating threats in the future.

To the question of the trend, Shaun, I don't see any -- I don't see the vulnerability of U.S. critical infrastructure peaking. I just see it going up and up and up, because we continue in many of the parts of critical infrastructure to rely more and more on information technology. And as we think about things like smart grid, if anything, the trend lines are going toward acceleration. At the same time, within the private sector and critical infrastructure in general, there is some good work being done, and I'd just like to encourage Congress and the administration to continue to pay attention, not just to the issue but to the technical work that's being done. And I think that we are within several years of being able to begin to

put in place much more effective technological solutions. Some advanced technologies, like I mentioned the Draper Lab example of the inherently secure processor and APL doing some of the work. In some retro tech, which could be selectively. So electromechanical switches rather than IT. And we've got to bring that framework more to bear. I've seen it happen in areas of critical infrastructure. I've seen it discussed more than implemented.

And finally, I think the other panelists will know more about the specifics about voting infrastructure than I do, but I'll just say it's a fundamentally important question. And we are headed into the next midterm sooner than one thinks. And again, the defensive posture is going to be fundamental to raising the threshold and reducing risk, as well as we should be making some strong public statements about consequences. And I don't think this time around that telling President Putin to cut it out is going to be sufficient.

MR. O'HANLON: Bill, Sam, or Anil, we can go down the row.

MR. LEIGHER: Yeah, I'd like to go back to the deterrence issue because there are some key differences in the DSB report. You know, one of the examples was malware that's been planted inside of a power plant. And to get to something like declaratory policy that we will respond when you discover something like that, I don't think we know how to think through that problem exactly yet, because I think you have to walk down the analogy of what it would look like on the kinetic side. You're going to say, well, don't target my power plants as part of your kinetic campaign, and we wouldn't agree to that. But when I discover that malware, is it vandalism? Is it trespassing? And we don't have a model for many of these things that happen in the cyber realm to understand yet. And I think it bleeds into the question. We're really going to have to get some experience, probably learn the hard way before we really understand what our tolerance is to act in a preemptive way or respond when you find, you know, these kind of attacks.

To the voting question, you know, I think, you know, we've given up so much of our rights and our privacy to the Internet, and it goes back to what I said in my opening. You know, what's the biggest problem? We don't design well. I think there are technologies now that -- block chain, you know, comes to mind, you know, off the top, that if you secure many of your transactions things, and voting is a transactional event, there are ways to do that. We do it with credit cards, and there's a lot of credit card

fraud, but we have a fundamentally secure way of dealing with individual transactions. And I think anything that we trust we have to do that. We have to have identity in a way that is probably better than we accept now and find transactional means that allow us to have secure voting at really big scale.

MR. O'HANLON: Thank you.

Sam?

MR. JONES: Yeah. So I'll just quickly respond to the voting related and paper printout questions. Less so on kind of those subjects. But on the printing out classified information and then keeping it only on paper, you're essentially describing the most extreme version of network segmentation possible. You know, if it's true, then the Russians are assuming that they're completely compromised, and if there's an attacker on their network, there's no way they can get access to that information because it's literally not on the network. A less extreme version is having different air gaps networks which is, you know, things are still, you know, on a network, but you can't get from one network to another. And a less extreme version would be if you have really good controls in place on your network, you know, maybe it's a PCI part of the network. If you're a retailer or something, the average person should not be able to get to this other part. I think there are circumstances for using all of those, but I would kind of view them as the same and just describe a very extreme version of it.

For the ballots, you know, less commenting on the actual issue, but this is kind of more of a joke, but I feel like I lose every other thing that gets mailed to me anyway. But at the same time, almost every Google employee can access all of their applications straight over the Internet. So there's like totally different risks when looking at those different problems. I'm not advocating for either one. I'm just saying, you know, we need to think about, you know, the approaches of both.

And then on the increased vulnerability side, one way to think about it is every new line of code that's deployed, either at the nation or at the enterprise has some proportionate amount of risk that's associated with it. Maybe it's linear. Maybe it's exponential. I don't know. That might be an interesting research project. But what we really need to do is try to lower either, you know, certain factors in that equation or the actual exponent, which would come through better design because, you know, everything is going to be networked and so the vulnerabilities will inherently only increase unless we like really change how those things are related.

MR. O'HANLON: Thank you.

Anil?

MR. RAMCHARAN: So speaking on the thought there, building on your comments around risk management, there becomes this tradeoff between functional capability and security. Jim, I think you said the safest computer is the one that never gets turned on. Information sharing is a part of how we operate, whether it's joint forces, coalition forces, or even internal federal government. Information sharing is foundational to operational capability. So being able to take that offline inhibits operational capability. So there's that tradeoff of where's that risk threshold where we're willing to say chance of compromise enables greater mission capability so it's a greater benefit than it is to take it completely offline. I think that's a constant decision that's being made both in the operational environment and even broader than that in terms of what's the appetite and tolerance for risk in that type of environment? I'd even say building on the concept of implanting things like risk management frameworks and decision processes is part of the cyber defensive posture and the operational environment is part of understanding how to address that type of decision space. Hopefully a priori (inaudible) is looking to push some of that. So in that context, I think that's an active conversation that's happening both within the federal space and within the military operations.

MR. O'HANLON: Two points I'll add on that and then we'll have one last question to wrap up with any concluding thoughts people may want to address as well or mention and include.

Of course, 15 years ago, 16 years ago, we were having a debate about how to make sure that we shared information in the aftermath of the 9/11 attacks when the stove piping of information within certain agencies prevented people from "connecting the dots," which this purported system, you know, of going back to just hard copy would exacerbate many times over. So obviously we have multiple security threats and concerns. And making computers just talk to a small group within their own agency or what have you would make a lot of other problems much worse.

And then, of course, Jim mentioned air-land battle, and we have a number of derivatives since then where fighting in real time, connecting sensors to shooters requires a network. There's just no other way about it. So you may try to make that network air gapped or some other way protected but you can't eliminate it unless you want to go back to the kind of kill probabilities and unit isolation that we had

in previous wars where, you know, things were astronomically less effective than they are today.

Now, obviously, if the system truly does break down, you're probably worse off for having created dependency and expectation upon it that you can no longer benefit from, but that's a pretty stark and extreme example.

So great question. I'm glad you raised it. But I don't see how we can go back to a paper system myself.

Sir, very last question and then we'll wrap up.

MR. SAREEN: Thank you. My name is Bimal Sareen Sheree and I'm a cofounder of Cyber Force NOC, which is a solutions and services company for critical infrastructure.

My question I think for the panel is what is your perspective on the differences in the government regulation and compliance for critical infrastructure? For example, the electric power utilities have a different set of regulatory requirements and enforcement requirements than the others that are directly related to them, like the pipelines and the gas pipelines and other aspects, the hydro power, hydroelectric power, et cetera? So shouldn't there be a more uniform and urgent requirement for this?

And the second part of this is should there not be a more -- a different set of government -- private sector government collaboration when it comes to critical infrastructure? Because if the critical infrastructure is attacked in some way, the typical response would be, by the way, you're the private sector, we'll handle this our way. They are slightly different behind-the scene rules for the electric power grid but not for the others?

MR. O'HANLON: Why don't we start with Anil? We'll walk down this way and finish up.

MR. RAMCHARAN: Sure. So I take to that comment. Awareness I think is part of the challenge. We're learning more about how to address critical infrastructure vulnerabilities as we better understand how susceptible they are to cyberattack tactics, techniques, and procedures. So I do expect to see advancement in both of those areas, both in the traditional power grid as we embrace capabilities like smart grid and then transition those back to other parts of critical infrastructure. So I'd expect to see standards continually evolve. And from what I'm hearing across governments is that there is a healthy appetite for this public-private collaboration because there's a fine line between what's purely commercial and what's actually support towards public safety. And I think that's where you're going to see a lot of this

evolution of -- a lot of regulation is driven from public safety concerns that cyber is now an active part of that conversation for public safety.

MR. O'HANLON: Sam?

MR. JONES: The thing I'll add, less on the policy side, but I think your question raised a lot of points about accountability. So who's actually in charge of defending this thing, which we've already been touching on before about, you know, the cyber commander that says that's not my job? Looking at behavior in like the typical enterprise and how they defend. If you don't have an accountability system, nothing gets done. So I think the first step is probably looking at who's actually, you know, in charge, who will get fired, and setting those in place before you even start thinking about policy.

Mr. LEIGHER: I think to follow with the first comment, there needs to be something that comes into the industrial sectors with critical infrastructure that you're really doing something akin to penetration testing and red teaming that we look at on a regular basis. I think that the change from -- in DOD from certification accreditation to adopting NIS risk management framework has been a step in the right direction. But again, I'll go back to they are mechanical engineers designing this, not cyber engineers. They're going to do, I think, the minimum and there needs to probably be more regulation on top of it to get the rules and the enforcement of the rules heading in the right direction.

MR. O'HANLON: Finish up.

MR. MILLER: On the question of regulation, I agree that more should be done for the most critical of the critical infrastructure, and I agree with your premise that -- not just that some is more critical than others but that there is a high degree of interdependency among some of the most critical, including electricity, gas, and water in terms of their operation. That said, I think that regulations should aim to give incentives and rewards as well as punishments. And there was a proposal put forward by the Obama administration. The original version of that emphasized that heavily. The chamber ended up opposing it. I never quite understood what was so wrong with it but I think it's important that while you want the entities to internalize the externalities of the risks and costs associated with a weak defensive posture, that to do it by rules and so forth rather than incentives is likely to be a costly and ineffective process because the adversary is going to adapt quickly and want to give incentives for -- our potential adversaries will adapt quickly. We want to give incentives for the owners and operators of these critical

infrastructures to do the same and to try to put it down in terms of a clear simple ruleset is not going to work well.

And then a final comment on the question of public-private partnerships, I think there's been some very good thought on this. I think a lot more needs to be done. And I'll just highlight two issues that to me are particularly interesting. One is the question of hack back. Illegal in the United States, although there's now consideration to make it legal in some circumstances. I'd be very reluctant to go that direction personally. But part two then is what authorities and presence could there be that could allow national or state authorities to be present. So as an example, we have a number of cyber mission teams that are National Guard. If you have a group that includes civilians, National Guard, reservists, and potentially active duty that's involved in monitoring and potentially response, you can have them turn their hats from Title 10, Title 50, Title 32, private sector, and so forth. And I think we need to really explore that model much more and look to thinking it through, gaining it out, and then applying it in some pilot programs where we really aim to increase the speed of innovation and the speed of response.

MR. O'HANLON: Sir? Why don't I give you 15 seconds just to go ahead and say what you wanted to say and then need to wrap up?

MR. EGGERS: Sure. I figure it would be worth just at least, since I'm sitting here I thought I'd help you out.

Matthew Eggers, U.S. Chamber of Commerce.

So in terms of our pushback on regulatory legislation from a few years ago, I figure I didn't want to miss an opportunity to suggest at least three things.

One, it's not clear that the regulatory approach could keep up with the threats. Two, we've seen where industries, such as financial services when regulated are heavily burdened by compliance rather than using resources towards optimal purposes. Three, we're trying to push very actively -- we've got a national campaign, domestically and increasingly overseas -- to push the framework. I would also maybe just finish by saying that many sectors -- financial services, electric, chemical, and so forth -- are regulated already. I would encourage stakeholders to spend time, an hour or two, with each sector, hear things that you want to hear, hear things that you don't want to hear. One thing we'd like to see happen is more public-private cooperation in the area of IOT security. That would

be a good thing. We're trying to lead that effort. More I think needs to be done, but anyway, I just wanted to say thank you, and I figured I'd throw in that plug for our position.

MR. O'HANLON: Thanks.

MR. MILLER: Thank you. I'd like to follow up with you separately, and interestingly, I find myself in agreement with your issues. The piece that I would most like to see is a standard of aggressive red teaming, not just pen testing but red teaming that's intended to take down critical infrastructure and an expectation that the owners and operators of critical infrastructure undertake that -- have that red team undertaken and then they have a plan for responding to it over time. If that alone were done, I think it would be a substantial step. And I know in some sectors that has begun to happen and I applaud that. I'd encourage you to see if you can pour some gasoline on that fire.

MR. O'HANLON: Well, listen. Thank you all for being here, and please join me in thanking the panel.

(Applause)

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2020