

[H.A.S.C. No. 114-50]

**OUTSIDE PERSPECTIVES ON
THE DEPARTMENT OF DEFENSE
CYBER STRATEGY**

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

HEARING HELD
SEPTEMBER 29, 2015



U.S. GOVERNMENT PUBLISHING OFFICE

97-196

WASHINGTON : 2016

COMMITTEE ON ARMED SERVICES

ONE HUNDRED FOURTEENTH CONGRESS

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

WALTER B. JONES, North Carolina	ADAM SMITH, Washington
J. RANDY FORBES, Virginia	LORETTA SANCHEZ, California
JEFF MILLER, Florida	ROBERT A. BRADY, Pennsylvania
JOE WILSON, South Carolina	SUSAN A. DAVIS, California
FRANK A. LOBIONDO, New Jersey	JAMES R. LANGEVIN, Rhode Island
ROB BISHOP, Utah	RICK LARSEN, Washington
MICHAEL R. TURNER, Ohio	JIM COOPER, Tennessee
JOHN KLINE, Minnesota	MADELEINE Z. BORDALLO, Guam
MIKE ROGERS, Alabama	JOE COURTNEY, Connecticut
TRENT FRANKS, Arizona	NIKI TSONGAS, Massachusetts
BILL SHUSTER, Pennsylvania	JOHN GARAMENDI, California
K. MICHAEL CONAWAY, Texas	HENRY C. "HANK" JOHNSON, JR., Georgia
DOUG LAMBORN, Colorado	JACKIE SPEIER, California
ROBERT J. WITTMAN, Virginia	JOAQUIN CASTRO, Texas
DUNCAN HUNTER, California	TAMMY DUCKWORTH, Illinois
JOHN FLEMING, Louisiana	SCOTT H. PETERS, California
MIKE COFFMAN, Colorado	MARC A. VEASEY, Texas
CHRISTOPHER P. GIBSON, New York	TULSI GABBARD, Hawaii
VICKY HARTZLER, Missouri	TIMOTHY J. WALZ, Minnesota
JOSEPH J. HECK, Nevada	BETO O'ROURKE, Texas
AUSTIN SCOTT, Georgia	DONALD NORCROSS, New Jersey
MO BROOKS, Alabama	RUBEN GALLEGU, Arizona
RICHARD B. NUGENT, Florida	MARK TAKAI, Hawaii
PAUL COOK, California	GWEN GRAHAM, Florida
JIM BRIDENSTINE, Oklahoma	BRAD ASHFORD, Nebraska
BRAD R. WENSTRUP, Ohio	SETH MOULTON, Massachusetts
JACKIE WALORSKI, Indiana	PETE AGUILAR, California
BRADLEY BYRNE, Alabama	
SAM GRAVES, Missouri	
RYAN K. ZINKE, Montana	
ELISE M. STEFANIK, New York	
MARTHA MCSALLY, Arizona	
STEPHEN KNIGHT, California	
THOMAS MACARTHUR, New Jersey	
STEVE RUSSELL, Oklahoma	

ROBERT L. SIMMONS II, *Staff Director*
KEVIN GATES, *Professional Staff Member*
LINDSAY KAVANAUGH, *Professional Staff Member*
NEVE SCHADLER, *Clerk*

CONTENTS

	Page
STATEMENTS PRESENTED BY MEMBERS OF CONGRESS	
Langevin, Hon. James R., a Representative from Rhode Island, Committee on Armed Services	2
Thornberry, Hon. William M. "Mac," a Representative from Texas, Chairman, Committee on Armed Services	1
WITNESSES	
Bejtlich, Richard, Chief Security Strategist, FireEye, Inc.	3
Delfino, Dominick, Vice President, World Wide Systems Engineering, Networking and Security Business Unit, VMware, Inc.	6
Schmidt, Dr. Lara, Senior Statistician, Associate Director, RAND Project Air Force, RAND Corporation	8
Wallace, Ian, Senior Fellow, International Security Program, and Co-Director of the Cybersecurity Initiative, New America Foundation	5
APPENDIX	
PREPARED STATEMENTS:	
Bejtlich, Richard	43
Delfino, Dominick	62
Schmidt, Dr. Lara	77
Wallace, Ian	54
DOCUMENTS SUBMITTED FOR THE RECORD:	
[There were no Documents submitted.]	
WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING:	
[There were no Questions submitted during the hearing.]	
QUESTIONS SUBMITTED BY MEMBERS POST HEARING:	
Mr. Shuster	95
Mr. Walz	96

OUTSIDE PERSPECTIVES ON THE DEPARTMENT OF DEFENSE CYBER STRATEGY

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
Washington, DC, Tuesday, September 29, 2015.

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” THORN- BERRY, A REPRESENTATIVE FROM TEXAS, CHAIRMAN, COM- MITTEE ON ARMED SERVICES

The CHAIRMAN. The committee will come to order.

Cyber is deeply ingrained in virtually every facet of our daily lives, at work, at home, in our schools, and in government. We are incredibly dependent upon it, and therefore we are incredibly vulnerable to disruptions or attacks that affect it.

Cyber is a great enabler for our daily lives, but the threats also pose a significant danger to our national security as well. What adds complication is that various estimates show 85 percent of the infrastructure that needs to be protected is owned by the private sector. And so the role of government in protecting not only itself, but the country in this new domain of warfare is a major challenge for us.

So that is part of the reason this committee is devoting a week to cybersecurity issues. We are starting today with an outstanding panel of experts to not only share their insights, but set up the discussion for the remainder of the week. Tomorrow we will have the deputy secretary of defense and the commander of CYBERCOM [U.S. Cyber Command] before us. The Emerging Threats and Capabilities [ETC] Subcommittee has a classified briefing on cyber later in the week.

Cyber, of course, is normally in ETC’s jurisdiction, but because it does translate to all aspects of this committee’s work and because of these overall policy issues, the full committee is having these hearings today and tomorrow.

As I say, there are a number of questions. What is the role of the Federal Government in defending that 85 percent of the infrastructure? How do you have deterrence in cyberspace? Do we have the necessary authorities and rules of engagement to engage in cyber warfare? Are we acquiring the people and the capabilities that we need? Do we have a strategy that can deal with what some of our adversaries are doing? What effect do things like the agreement that the Chinese and the President have reached this week have on cyber? Just some of the questions for us to explore.

So I really appreciate to start off our cyber week having this outstanding panel of experts. Before we turn to them, I am going to yield to the distinguished ranking member of the Emerging Threats and Capabilities Subcommittee, Mr. Langevin, for any comments he would like to make.

STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, COMMITTEE ON ARMED SERVICES

Mr. LANGEVIN. Thank you, Mr. Chairman.

And thank you to our witnesses for appearing before us today on the Department of Defense's new Cyber Strategy released in April 2015. I certainly look forward to hearing what you have to say.

Ranking Member Smith is going to be joining us a little later today, so I will be delivering a synopsis of his remarks on his behalf.

So I look forward to hearing the witnesses' perspectives on the five strategic goals, their views on the objectives outlined in the strategy in order to achieve those goals, and what else we should be thinking about to improve the posture of the Department of Defense [DOD] in the cyber domain.

Cybersecurity is an issue that the chairman, the ranking member, and I have been focusing on throughout our tenure on the Armed Services Committee. Our time on the Emerging Threats and Capabilities Subcommittee has given us all insight into what has been recognized since 2013 by the Director of National Intelligence as the number one strategic threat to national security. We have worked in coordination with the Department of Defense across the whole of government and with the private sector for many years to better enable the country to deter, defend, and respond to cyberattacks.

Despite best intentions, as a nation we are not keeping pace, though, with the sophisticated and ever-evolving cyber threat. The DOD has made progress. But as Admiral Mike Rogers noted in his June 2015 Vision and Guidance for the U.S. Cyber Command, I quote: "The Department is still in the very early stages of harnessing the power of our Nation's cyber enterprise."

I believe the new Cyber Strategy will better guide the Department in its efforts to harness the cyber enterprise. The five strategic goals—building and maintaining ready forces and capabilities; defending the network, securing data and mitigating risk to missions; being prepared to defend the homeland and U.S. vital interests from cyberattacks of significant consequence; building and maintaining a viable cyber operations, and plan to use those options to control conflict escalation and shape the conflict environment; and building international alliances and partnerships to deter and increase stability—set the stage for the U.S. to gain an advantage across the cyber domain, an advantage we desperately need, as evidenced by the recent hack of the Joint Staff unclassified network.

Yet, not all of these goals and objectives are necessarily new concepts. Many are significant issues that Congress and the Department have discussed for years. Yet, execution of the objectives has presented technological, policy, and doctrinal challenges at the tac-

tical, operation, and strategic levels. The new strategy provides us an opportunity to confront and address those challenges so our goals can become reality sooner rather than later.

For instance, we know the Department needs qualified military and civilian personnel in order to build and maintain forces to conduct cyber operations. But how does the Department compete with the private sector for highly skilled individuals, especially in a budget-constrained environment.

This committee has also been hearing about the necessity for an effective cyber deterrence strategy for several years. Time has shown the need for such an effective policy has only grown, but we are still grappling with how to approach deterrence given the difficulty of attributing attacks and the overall strategic implications of such a policy. So deterrence requires us to relook at the way we tend to think about warfare, about what constitutes an act of war.

I look forward to the witnesses' views on this issue, as well as how we can operationalize other aspects of cyber. These are just a few of the issues that I hope that we will examine today.

Chairman Thornberry, I want to thank you for holding this hearing. I know of your commitment and interest in cyber issues, the work that we have done together both on the Emerging Threats and Capabilities Subcommittee and our many years together on the House Permanent Select Committee on Intelligence have given us particular insights into the challenges in this space. And, again, I appreciate the attention that the full committee is giving to this issue this week.

With that, I thank the chairman. And I yield back.

The CHAIRMAN. I thank the gentleman. He is exactly right, he and I have grappled with this issue for a number of years. And I very much appreciate Chairman Wilson and the gentleman from Rhode Island in their efforts to pursue this at the subcommittee level. And, certainly, the full committee is not and cannot replace that diligence that they bring to this important issue.

Let me, again, welcome our witnesses. We have Mr. Richard Bejtlich, chief security strategist for FireEye; Mr. Ian Wallace, senior fellow and co-director of the Cybersecurity Initiative at the New America Foundation; Mr. Dominick Delfino, vice president at VMware; and Dr. Laura Schmidt at the RAND Corporation.

I appreciate the written testimony that each of you have submitted. I have read it. And I will ask unanimous consent to have that included in the record. Without objection.

And so, if you would please, summarize your testimony before us, and then we will turn to questions.

Mr. Bejtlich, if you would like to begin.

**STATEMENT OF RICHARD BEJTlich, CHIEF SECURITY
STRATEGIST, FIREEYE, INC.**

Mr. BEJTlich. Chairman Thornberry, Ranking Member Smith, distinguished members of the committee, thank you for the opportunity to testify. I am Richard Bejtlich, chief security strategist at FireEye. I am also a nonresident senior fellow at the Brookings Institution and I am pursuing a Ph.D. in war studies from King's College, London. I began my security career as a military intel-

ligence officer in 1997 at the Air Force Information Warfare Center.

Speaking today as a FireEye strategist and as a former military officer, I assess the new DOD Cyber Strategy as a transition document. Previous strategies emphasized DOD's role as protecting DOD networks from attack. The current document restates this role and adds a new, albeit limited, mission to, quote, "defend the U.S. homeland and vital interests from disruptive or destructive cyberattacks of significant consequence."

Stepping outside the beltway for a moment, it might be natural to ask what about OPM [Office of Personnel Management] or even what about Sony. For these reasons, I believe DOD's strategy is a step in the right direction, but one that needs to be augmented by additional measures.

Now, at this point in my written remarks I cover four associated topics: Private sector security capabilities, attribution, hack-back, and acquisition. But in order to meet my time limit, I respectfully refer you to those written documents. And here I would like to turn straight to five recommendations to improve the Nation's digital security.

First, I recommend that DOD and the Intelligence Community modify the nature of offensive digital operations against national adversaries. According to open source intelligence tradecraft and stories published in open media, U.S. Government offensive digital activities currently focus on traditional espionage targets. These operations fulfill collection requirements such that U.S. Government decisionmakers can execute their duties based on accurate and actionable intelligence.

Foreign intelligence services also conduct these operations. However, foreign intelligence services, military units, and other teams also attack private sector companies in this country and elsewhere. They also attack civil society organizations and even individuals.

U.S. offensive digital capabilities should therefore be ordered to directly target the foreign teams that are attacking private U.S. entities. By putting pressure on these foreign teams, U.S. victims would receive some relief from the relentless waves of foreign hacking campaigns. By pressure, I mean low-level activities that introduce friction and uncertainty into the minds and processes of foreign hackers.

For example, U.S. offensive teams could quietly corrupt tools and infrastructure used by foreign teams against domestic targets. They could periodically crash foreign computers used to hack U.S. targets or degrade bandwidth used to transport malicious traffic. The idea is to introduce obstacles into foreign hacking operations such that they are working uphill when trying to attack U.S. victims.

Second, the DOD, the IC [Intelligence Community], and partners should consider indirect ways to help protect U.S. private sector and associated targets. If government actors learn that private entities are being targeted by a foreign adversary, they should be more willing to warn of the attack before it happens. Our current strategy is essentially we tell the victim after they have been hacked, which that is valuable, many times that is the only way a victim learns, but we need to know earlier in the process.

Third, I recommend that the Congress and DOD should sponsor a study into creating an independent cyber force. As a former captain who performed the computer network defense mission in the Air Force, I am very pleased to see the existing military services improving the career paths and opportunities for today's troops. For example, I spoke at an Army Cyber Institute event last week and I watched two young Army captains explain how they would apply cyber tactics to a simulated physical combat mission.

Unfortunately, I was reminded of the challenges facing these young officers when an audience member warned that the pair's noncyber colleagues might, quote, "think they were playing warrior," and that their makeshift technical solutions might appear to be a toy. These cultural barriers are real and inherent in each military service's ethos.

Fourth, and this is stepping outside DOD a little bit but it affects the entire government, I recommend that the President appoint a U.S. chief information security officer or U.S. CISO. The executive branch already has a U.S. chief information officer [CIO] and a chief technology officer [CTO]. This is similar to the situation of many private sector businesses before a breach, but after a breach they quickly change. Thus far, the government has not changed. We still don't have a U.S. CISO. And I would put that person at the level of current U.S. CTO and U.S. CIO personnel.

Finally, I recommend the administration should develop the capability to take asymmetric actions that target adversary core interests, but in a way that leverages our strengths against their weaknesses. In my written statement, I discuss one example involving China's Great Firewall.

I look forward to answering your questions.

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

The CHAIRMAN. Thank you.

Mr. Wallace.

STATEMENT OF IAN WALLACE, SENIOR FELLOW, INTERNATIONAL SECURITY PROGRAM AND CO-DIRECTOR OF THE CYBERSECURITY INITIATIVE, NEW AMERICA FOUNDATION

Mr. WALLACE. Chairman Thornberry, Ranking Member Smith, distinguished members of the committee, thank you for inviting me to testify about the Department of Defense's strategy for cybersecurity. I am Ian Wallace. I am a fellow in the International Security Program at New America. And I am the co-director of New America's Cybersecurity Initiative.

As I set out in my written testimony, the DOD's strategy is a necessary and welcome update to the 2011 Strategy for Operating in Cyberspace. And as such, I think it does a good job of identifying and describing the actions that will be necessary for the DOD to meet the challenges it faces today. And it also, I have to say, shows an admirable new level of transparency in the way that the DOD discusses these issues.

But no strategy is perfect, and in my written testimony I offer two particular ways in which I think the committee can usefully help the DOD improve on the strategy. The first of these will be to ensure that the DOD does not fall into the trap of becoming the

default choice for responding to threats against the Nation's civil infrastructure. The second will be to ensure that despite the undoubted cyber threat that the United States faces today, the DOD is also properly thinking about the future operating environment in which U.S. forces will fight.

Both these points are important. But while the immediacy of the current threats are alarming and the issues like deterrence and attribution undoubtedly deserve further discussion, I encourage members not to lose sight of my second point.

To understand the importance of thinking ahead about the implications of new technology, let me for a moment offer the analogy of the advent of military aviation. My own country, Britain, emerged from the First World War as a leader in carrier aviation. By the beginning of the Second World War, Britain had been eclipsed by the United States, and this new capability was obviously crucial in America's prosecution of that war.

There were a number of reasons for this, but they include United States willingness to do four things that are highly relevant to our current situation. Those four things were the willingness to engage in operational experimentation, a willingness to actively foster new thinking about operational concepts in the top military educational establishments, a willingness to make big organizational changes based on those new concepts, and perhaps most importantly, a willingness to encourage the best and brightest—that includes the likes of Halsey, Nimitz, and King—to make this new technology central to their careers.

History does not repeat itself exactly. In the 21st century, the DOD's response to new cyber capabilities will need to be much more joint than the approach taken in the 1920s and 1930s. But now, as then, longsighted action and the support, even active pushing of Congress, will be crucial to maintaining the United States military edge in future military operations.

I look forward to your questions.

[The prepared statement of Mr. Wallace can be found in the Appendix on page 54.]

The CHAIRMAN. Thank you.

Mr. Delfino.

**STATEMENT OF DOMINICK DELFINO, VICE PRESIDENT,
WORLD WIDE SYSTEMS ENGINEERING, NETWORKING AND
SECURITY BUSINESS UNIT, VMWARE, INC.**

Mr. DELFINO. Chairman Thornberry, Ranking Member Smith, and members of the committee, thank you for the opportunity to testify today on the Department of Defense's Cyber Strategy. I am Dominick Delfino, vice president of World Wide Network and Security Systems Engineering at VMware. I ask that my full statement be submitted for the record.

We believe that the DOD Cyber Strategy is a good first step toward improving the Department's cyber posture. However, as with any strategy, the complexity is in the execution of the implementation. With respect to goal number one, building cyber-ready forces and capabilities, VMware believes that this challenge can be managed with industry-proven practices, such as using technology that is available today to mimic currently evolving threats. Once in

place, these cyber classrooms can provide on-demand training to warfighters globally.

We also recommend that DOD leverage automation technologies to simplify cyber detection. By automating responses that can be just as rapidly undone, the Department can empower today's network professionals with the ability to stop threats immediately without having to wait for complex systems changes.

For recruiting experienced personnel, the Department should consider using programs like the government's special hiring authority that is used to pay higher wages for people who have specialized skills. We also recommend creating a clear promotion path to command-level responsibility for cyber warriors.

For goal number two of the Cyber Strategy, defending the DOD information networks, we believe a new approach to network architecture is needed. As we have seen in the recent private sector and government attacks, hackers were able to penetrate perimeter systems and gain access to networks where they were free to access and steal sensitive data over a period of several months.

Hackers typically use this attack methodology because traditional perimeter-centric security systems are structurally designed to be doors to the network. These doors serve to allow authorized users access to network systems and to prevent unauthorized users from getting inside the network. Once the intruder has penetrated perimeter security, there is no simple means to stop malicious activity within the data center without extreme disruption to the government's mission.

For example, imagine a street with homes on it as an analogy for a network with servers in a data center. Let's assume there is a corridor that connects every home on the street. If an intruder can manage to break into one home, the intruder now has complete access to all of the other homes on the street, even though their doors to the street are locked, because there is a trusted passage between them. In technology terms, the larger and the flatter the network and the more servers on the network, the higher the probability the hacker will be able to penetrate one server and leverage it to compromise others on that same network.

In order to prevent an attacker from moving freely within the network, the Department should compartmentalize its networks, implementing what is called a Zero Trust or micro-segmented environment. A Zero Trust environment prevents unauthorized movement by minimizing the attack surface of the network. When a user or system breaks the rules, the potential threat incident is compartmentalized and security staff can take any appropriate defensive actions. This limits the intruder's ability to move around freely within the network and significantly mitigates the impact of a successful perimeter breach. This approach is being widely adopted by the commercial sector, including the financial industry and some areas of the government.

We applaud the Department's efforts to move towards the Joint Information Environment [JIE] and believe if done correctly it will significantly enhance the cyber posture of the DOD. We believe that the DOD should leverage the existing cloud technologies it owns and consolidate those workloads to move into the JIE first, measuring success through a scorecard. We also recommend the

Department review how it treats unclassified business systems. Currently these systems, such as email, personnel, and payroll, are treated differently than classified mission-critical systems under current DOD practices.

Finally, for goal number three, defending the homeland from cyberattacks, we recommend two approaches in addressing these initiatives. The first is to automate security features. This will allow the Department to proactively deploy countermeasures. The second approach is to use predictive methods to quantify attacks and likely actions based on their early stage. Investing in these capabilities will yield significant benefits by preventing later-stage and more serious attacks based on the precursor activities.

In summary, when implementing its Cyber Strategy, we believe the DOD should establish aggressive goals for automating the management of its IT [information technology] infrastructure security controls. The Department should also cut the common thread linking every major breach by implementing a Zero Trust security model to reduce attacker and threat mobility within the network. Finally, the Department should implement a scorecard to aggressively and manage each command's progress towards moving to the JIE.

Thank you for the opportunity to testify today. I look forward to answering any questions the committee might have.

[The prepared statement of Mr. Delfino can be found in the Appendix on page 62.]

The CHAIRMAN. Thank you.

Dr. Schmidt.

**STATEMENT OF DR. LARA SCHMIDT, SENIOR STATISTICIAN,
ASSOCIATE DIRECTOR, RAND PROJECT AIR FORCE, RAND
CORPORATION**

Dr. SCHMIDT. Thank you. Chairman Thornberry, Ranking Member, and members of the committee, I am honored to be here today to discuss this important topic. My name is Lara Schmidt and I am a senior researcher at the RAND Corporation.

As I described in my written statement, the 2015 DOD Cyber Strategy clearly defines DOD's missions in cyberspace, and as is typical for a strategy, establishes several goals to ensure DOD is able to accomplish these missions. The goals are: to build and maintain ready forces and capabilities to conduct cyber operations; to defend DOD networks, secure DOD data, and mitigate risks to DOD missions; to build and maintain viable cyber options and plan to use them in the range of conflict scenarios DOD may face; to be prepared to defend the homeland and U.S. vital interests from cyberattacks of significant consequence; and finally, to build and maintain international alliances and partnerships to deter threats and increase stability and safety, security. The strategy also identifies a series of implementation objectives to achieve these goals.

With all that said, I have four main points I would like to share with you about the 2015 DOD Cyber Strategy. First, a capable cyber workforce is critical to achieving the goals laid out in the strategy. But the commercial sector is also vying for high-quality personnel with the same skill sets. However, DOD has an opportunity to learn from the commercial sector to attract capable mili-

tary, civilian, and contractor personnel. Research into commercial hiring and retention practices shows that for most of this workforce, it does not all come down to pay, and even on that scale, DOD is not as bad off as many fear.

The one exception is the market for the few personnel with elite cybersecurity skills, these so-called ninjas, who are a competitive advantage for cybersecurity and other firms and as a result, command large salaries.

My second point, despite the excitement surrounding DOD offensive and defensive cyber operations, it is important to remember that the bulk of the workforce is involved in the critical job of configuring and maintaining DOD hardware, software applications, and networks around the world. Ensuring the continued functioning of these systems and networks, even in the absence of cyberattack, is crucial. Therefore, this DOD IT workforce, or as DOD calls it the DODIN [Department of Defense Information Network] workforce, requires continued support as well.

Third, DOD has adopted a risk management approach to securing its systems across their life cycle, and this is commendable. However, it is a challenging undertaking due to the scale of DOD systems and networks, the ever-changing cyber threat, and the hard choices that will need to be made to prioritize risk mitigation efforts. Adequate resources and practical approaches need to be brought to bear to effectively implement the risk management framework.

Fourth, the strategy seeks to integrate cyber operations, including offensive operations, into military plans for all stages of conflict. In order to do this, the Department must take a scientific approach to evaluating whether offensive cyber capabilities will achieve the intended effects when called upon and avoid unintended effects. Doing so requires significant rigorous testing, data collection, and analysis efforts.

So in conclusion, it is my view that the DOD Cyber Strategy lays out an ambitious set of goals that are well aligned to operationalizing cyber. However, implementing the initiatives needed to achieve these goals will be challenging due to the difficulties in quickly building and maintaining a capable workforce, assessing risk across the large number of DOD networks and systems, and planning for operations in this highly dynamic environment. Achieving the goals of the strategy will take time and significant resources. I appreciate the opportunity to discuss this topic and I look forward to your questions.

[The prepared statement of Dr. Schmidt can be found in the Appendix on page 77.]

The CHAIRMAN. Great. Thank you. I appreciate all of you all being able to get a lot into a short amount of time in your oral statements. But, as I said, I appreciate your written statements as well.

I think a lot of notable historical figures have made the point that it is more important to get the questions right, in a way, than it is to get the answers, or at least you ought to spend more time and effort focused on what the proper questions are before you attempt to find the answers. So I would just like to ask each of you,

what is the primary proper question for us as policymakers to ask or to grapple with when it comes to cyber?

I have thought that maybe it was, what is the appropriate role of the military in defending the private sector infrastructure? Mr. Wallace kind of addressed that in his comments. But that may not be the most important question for us to ask. Maybe it is on the people side. Maybe it is something else.

So without trying to steer you in any direction, for policymakers, what do you think the most important question or issue for us to grapple with when it comes to cyber and our country's security?

Mr. Bejtlich.

Mr. BEJTlich. Sir, I would define it as, what is the acceptable level of loss for this country? For example, I don't want to equate the country to a store, but every store accepts a certain amount of shrinkage, in other words, theft from the store. We accept in the geopolitical realm a certain amount of instability. We have to define in this realm, what is it that we are willing to tolerate? You could argue simply by inaction we are tolerating quite a bit right now in terms of theft of intellectual property, theft of personally identifiable information. Essentially by inaction, we have determined that that is acceptable.

Now, do we want to push back on that and say, no, we are not going to accept that? I think the President has done a little bit of that now with China, although we can talk more about that. But that to me is the central question, what is the acceptable level of loss and how do you define that loss?

The CHAIRMAN. Okay.

Mr. Wallace.

Mr. WALLACE. As I mentioned earlier, I think the appropriate role of the military is an important question. The other important question that I think needs to be asked is, in a world where technology is effectively leveling out the differences between countries and their ability to engage against each other, how does the U.S., and particularly the U.S. military, maintain its advantage? And if that is no longer technology, I think the answer is likely to be in its ability to build alliances and in the quality of its people. But that doesn't happen by accident. That requires investment and forward planning.

The CHAIRMAN. Okay. Thank you.

Mr. Delfino.

Mr. DELFINO. I think the appropriate question is, how do we move from a stature of managing compliance to a stature of managing risk? Legislation can only be passed so frequently. And we are in a world where the dynamics of this is changing daily. And how do we really put a defensive posture in place and potentially an offensive posture in place that manages the risk with the association of potential DOD systems and infrastructure and military capabilities being breached?

The CHAIRMAN. Okay.

Dr. Schmidt.

Dr. SCHMIDT. I agree with Mr. Delfino. I think that the most important question in my mind is, how is DOD postured to protect its own networks, its own data, its own missions against the evolv-

ing cyber threat? And it all comes down in the strategy to the implementation plan of a risk-assessment approach.

The CHAIRMAN. Okay. I think there is more to pursue there, but I want to get to other members.

Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Again, I want to thank our witnesses for your very insightful testimony.

I guess I would like to start, first of all, with Mr. Bejtlich, on your call for a Federal CISO. And I have felt similar for quite some time and have had legislation in for years now calling for a director's position in the Executive Office of the President that has both policy and budgetary authority to reach across government to compel departments and agencies to do what they need to do to close our cyber vulnerabilities. Right now, we do not have anyone in charge, ostensibly, in that respect. The closest we have is the cybersecurity coordinator. It is a special assistant to the President position, but it is advisory and has no policy and budgetary authority. Not even the Secretary of Homeland Security doesn't even have the ability to reach across government and compel departments and agencies to do that.

So you called for a Federal cybersecurity officer. My vision had been that this director's position would apply mainly to the .gov domain. Are you suggesting that this Federal chief information security officer would have jurisdiction both over DOD operations as well as .gov or would you separate the two?

Mr. BEJTLICH. Thank you for the question, sir. I would separate the two. Traditionally in government IT we have carved out DOD and IC systems from the rest of the approaches. And in my experience, DOD and the IC are doing the best job as far as defending themselves.

They also have a unique culture in a sense that they do something called projecting friendly forces on the network. In other words, they assume that they are compromised and they are out there looking for the adversaries. This is a culture shift that needs to take place in the rest of the government, in the civilian side of the government.

And that would be my initial mandate to the Federal CISO, would be to bring that culture of going out there and looking for intruders in the Federal networks, as opposed to continuing to build higher walls. Which we do need to improve Federal security, there is no doubt, but you need to have two missions, finding the intruders and kicking them out and also improving security.

Mr. LANGEVIN. Good. Thank you.

So for the panel, when it comes to violence in the physical domain, society by and large manages to keep a lid on our worst impulses or at least has established a countervailing structure of rule of law. However, we seem to have a deficit of structures of a similar nature with sufficient influence over cyberspace, particularly supranational issues.

Moreover, it seems increasingly clear that we as a global society have a tactical deficit when it comes to defense in cyberspace. The Internet ecosystem is not solid defense and defense agility in equal measure to the offensive capabilities it unleashes.

Would you agree? And if so, how do we harness our S&T [science and technology] capabilities in our global influence to turn this picture around?

Mr. DELFINO. If I may, Congressman. I think an element of this has to be compared to terrorism, right? Cyberterrorism is analogous to terrorism. And our enemy only has to be right once and we have to be right every single time. So I think the effort that this Nation has put into dealing with the threat of terror within the Nation, we need to take similar aspects and attributes and efforts and put them into cyberterrorism as well.

Mr. LANGEVIN. Thank you.

Anyone else?

Mr. BEJTICH. Sir, if I could offer, when we think about risk as security professionals, we have three levers we can pull: There is vulnerability, there is the threat, and there is the consequences or cost of an intrusion.

In my community, the tactical community, we have spent way too much time, in my opinion, on the vulnerability side. It is important to reduce vulnerabilities, but we are moving to an Internet of things where there are tens of billions of devices on the Internet, and trying to reduce the vulnerabilities in all of them is just too much. Similarly, on the cost side, we increasingly have more and more information on the Internet.

So I do recommend that we do as much as possible to minimize. In fact, I saw Representative Buchanan has a bill to try to get rid of Social Security numbers on tax returns. I think that is a wonderful idea.

But the one part of that equation that is really not exploding—I mean it is growing, but not exploding—is the threat side. The head of Interpol the other day said that he estimates there are only about 100 malware kingpins in the world. These are the top-level guys who can write the worst malware for criminal purposes. A hundred of them compared to tens of billions of devices we have to secure. I would put much more emphasis on, as Mr. Wallace mentioned, working with our allies, going after those criminal groups. I think that would bring a little bit more security to the Internet.

Mr. LANGEVIN. Thank you.

My last question—and I will have others, but for right now given time constraints—it is no secret that the cybersecurity workforce is challenged and it can be difficult to mesh the private sector and the needs of government. Certainly the National Guard plays an important role in bridging that divide, and I am extremely proud to host the 102nd Network Warfare Squadron in the Rhode Island National Guard in my district. The Guard is and will remain a critical pathway for the DOD to access expertise that it otherwise, frankly, could not afford. It is an important model and one that has many variants. I am reminded particularly of Estonia, which has a cyber defense league operating under a volunteer paramilitary model.

Is the strategy being creative enough when it comes to ways to both integrate the capabilities of the Guard and access the capabilities of the private sector, be it through Secretary Carter's outreach to Silicon Valley, some paramilitary program such as Estonia's, or any other model?

Mr. WALLACE. I very much agree that the National Guard offers important opportunities for ways to involve people in the implementation of the DOD's strategy, experts that wouldn't otherwise be able to be used. But I do think we need more work to understand exactly how that will work in the future and avoid slipping into a situation where we militarize problems that don't necessarily need to be militarized.

There is a real question about how you spread responsibilities between civilian experts and military experts, and simply pulling the experts into the military isn't always the best solution. It may be the best way to deal with supporting warfighters in fighting wars, but in terms of defending civil infrastructure, one of the things we have to do is make sure that we better understand how the private sector and defense can work together.

Dr. SCHMIDT. If I could just add a few things. I think that your point about the National Guard and the Reserve Forces is an excellent one. They stand to provide the longevity that is required to maintain the technical depth that is necessary to perform these cyber mission roles. However, the question that I would ask is, are they well aligned with their expertise in their civilian sector jobs? Are they engaged in cyber activities there such that they can be bringing that expertise to DOD or are they doing completely different things in their civilian lives?

You also asked about the new—is the strategy being innovative enough, forward thinking enough to take on these new initiatives for getting the workforce that we need. And I think that one of the positive things that has happened lately has been the release of the new DOD Directive 8140, which basically aligns job roles with the knowledge, skills, and abilities that are required to perform those roles and identifies three separate categories of cyber-oriented jobs: an IT category, a cybersecurity category, and a cyber effects category. And this is the first time we have seen that kind of clarity coming out for workforce management. I think it stands to really align the training that is required to do those types of jobs and lay forward career progression that is an effective strategy for DOD.

Mr. LANGEVIN. Thank you, Dr. Schmidt.

Mr. Delfino, do you have any comment?

Mr. DELFINO. Well, I believe Dr. Schmidt covered most of my thoughts as well. I do believe that we need to have a consistent focus on recruiting the proper talent into those roles, whether they be military, civilian, Guard, reservists, et cetera, so on and so forth. And I do believe, as Dr. Schmidt outlined in her oral testimony, that the government can be competitive with the private sector marketplace, particularly when they target recruits and candidates who are early in career and use methodologies like we have in the ROTC [Reserve Officers' Training Corps] where we can actually offer scholarships to these individuals going into universities and partner with the right universities with the right academic programs in computer science, and then have them serve some mandatory period of time postgraduate in either a military or civilian capability to fight our cyber efforts.

Mr. LANGEVIN. Thank you.

Mr. Bejtlich, do you have any comment?

Mr. BEJTLICH. Yes, sir, quickly. I endorse Under Secretary Carson's work to make DOD more flexible. One of the things we should consider is being able to take an Active Duty person, have them work at FireEye for 2 years, we would love to have them, and then send them back to DOD. We need this fluidly to go back and forth between the private sector and the public sector.

Secondly, just as an issue with the Guard, I love the Guard, I have done some exercises with them. Sometimes they beat the regular forces at the fort. However, we have to be careful, some of those same people who are working in the Guard, if the flag goes up and they have to do DOD duty, they are not going to be around to defend Bank of America or another place that we really care about. So that is why I am partial to looking into a cyber force where we do have people whose job it is, if things get really bad, to take care of those bad problems.

Mr. LANGEVIN. Thank you, Mr. Chairman. I have other questions. But I will yield back.

The CHAIRMAN. Thank you.

Mr. Forbes.

Mr. FORBES. Mr. Chairman, first of all, I want to thank you for your leadership in this area and for having this hearing. I also want to thank Mr. Wilson for the efforts that his subcommittee is doing in this area and continues to do.

And as the chairman said, sometimes it is important for us to ask the right question. In this area, there are so many questions to ask and it is so big and so complicated. I would like to maybe narrow in on just one. Under the current DOD practices, unclassified business system networks, such as email and payroll, are not defended as strongly as classified networks.

Mr. Delfino, you have highlighted how an attack on an unclassified payroll system at DOD could impact the morale and families of DOD employees if the payroll system were to be compromised. You also mentioned an important point, that as the Department is implementing its network defense across the enterprise, it should review how it treats unclassified business system networks. As you know, these systems were recently the subject of a cyberattack.

Do you think that DOD should be treating unclassified networks any differently than classified networks? And what recommendations do you have for the committee to improve their cyber posture.

Mr. DELFINO. Thank you for the question, Congressman Forbes.

So I do believe while systems may be unclassified from a national security perspective or from a confidentiality perspective, they may be no less mission critical to the DOD or its efforts as well. And I don't believe they should be treated differently from a security posture perspective as it relates to its technology controls at all.

And many times these systems will, with less security, will be leveraged as a jumping-off point for a hacker. This happens in private enterprise many, many times. We have seen it happen in multiple government attacks as well. And they should be treated with the same model, they should be treated with the same security controls. Albeit they may be separated from the classified systems, it doesn't mean that there is a need for less security on those systems. As I referred to, a Zero Trust security model or a micro-seg-

mented security model would be one foundational aspect of how to secure these systems as well.

Mr. FORBES. We appreciate the expertise of all of our witnesses. Do any of you agree or disagree with Mr. Delfino in his assessment of the problem there?

Dr. SCHMIDT. I would just mention that the DOD is taking a risk-management approach to managing the security of their networks, and that requires not only understanding how the systems are going to be used and the vulnerabilities, but also the threats.

One of the large pieces of implementing a risk-management framework, though, is tracing what missions use what systems, whether it is a computer or a server or an integrated circuit somewhere deep within a weapon system, and understanding how those missions are dependent on the computer systems that could be attacked. It is a huge analytic effort, it is difficult, and it is something that DOD is going to have to grapple with.

Once they identify the risks to those systems, they would then protect them accordingly, and that is all part of a risk-assessment initiative. And I agree with your original statement that it doesn't necessarily depend on classification, it depends on impact to the mission.

Mr. FORBES. Thank you.

Mr. WALLACE. I would endorse the comments of Dr. Schmidt. I think in a risk-management approach some information will be inherently more sensitive than other bits of information. The trick in this new environment is understanding your risk and acting appropriately.

Mr. FORBES. Good. Thank you so much.

Well, thank you all very much.

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

The CHAIRMAN. Mrs. Davis.

Mrs. DAVIS. Thank you, Mr. Chairman.

And thank you all for being here and providing your outside expertise. We appreciate it.

You are all talking about risk management, risk assessment, and how important that is. I am wondering if you feel that we should be exploring or really where do you think that tools of deterrence fit and how are we developing those, how should we be developing those. What do you think makes sense?

Mr. BEJTLICH. Ma'am, I believe that there is a certain amount of deterrence in play now. There are actors who have the capability to cause substantial damage to different companies and organizations, and yet they don't. We have only seen a few examples. Sands Casino, apparently Iranian actors. Sony Pictures in the U.S., North Korean actors. There is plenty more that could be done, but it hasn't happened. So there is a certain amount of deterrence that is occurring.

The question, though, has been at the subdestruction level, the destruction of data, subphysical level, there has been a lot of activity, mostly in the form of theft of business secrets. Hopefully that will change. I am not sure if it will, but we will see.

Mrs. DAVIS. To what extent is the fact that we don't always know where things are coming from?

Mr. BEJTLICH. Well, ma'am, in my testimony I address attribution, and there has been a revolution in attribution over the last 5 years, both, I would say, in the government, but also in the private sector. Just last week, two security companies essentially revealed the entire life story of a Chinese hacker operating out of Kunming. This is something that would have taken me months to do in the military.

So the attribution problem, as more and more of our lives are online, those are hackers too, they are online, and we are finding out who these guys are even without having access to classified information. So attribution is much less of a problem than it was 5 years ago.

Mr. WALLACE. I would just like to build on Mr. Bejtlich's comments by adding that I think deterrence very definitely exists. But that deterrence of cyber threats doesn't have to happen within cyberspace.

One of the most significant deterrents for nation-states particularly to attack the United States is the fact that the United States is the biggest military power in the world and adversaries know that if they step over a certain line they will invite a response. That, as Mr. Bejtlich points out, pushes the threats down to the level where below that which the United States would be willing to go to war.

There are still tricky issues to manage, but to a large degree that counts as success and means that at least a good proportion of threats can be dealt with by other parts of government and the private sector themselves.

Mrs. DAVIS. Anybody else? Are you seeing that whole-of-government response to deterrence, though? Are we doing a very good job with that, bringing?

Mr. BEJTLICH. Ma'am, there have certainly been activities coming out of DOJ [Department of Justice] with the indictment of five PLA [People's Liberation Army] officers. I actually met with four PLA colonels several months after that happened and they were shocked that we had done that. So that has certainly played a role. I know that USTR [Office of the United States Trade Representative] has been looking at some activities. So different parts of the government have been trying to do this. The effects, though, are what I am waiting to see.

Mrs. DAVIS. Okay.

Dr. SCHMIDT. On the DOD end of things, you are talking about trying to change an adversary's decision calculus. So you can do that also by raising the costs. So efforts to improve the resilience of DOD systems is certainly something that you take into account in terms of deterrence, and also the advent of offensive operations that could be used to impose costs on the adversary and better defenses that just make it harder for the adversary to attack.

Mrs. DAVIS. Is there a role of sanctions in that as well?

Dr. SCHMIDT. Absolutely.

Mrs. DAVIS. Yeah. Okay.

One of the issues that we deal with here, and we had a discussion the other day about procurement, and, you know, the Department of Defense has had silo problems for years and people not really having that whole-of-government approach as well. But I am

just wondering, within the cyber community where adaption has to be so critical and so important and moving quickly in making those changes, how would you assess the Department of Defense in that regard, in this area?

Dr. SCHMIDT. I think one of the key ways that DOD isn't quite as adaptive as you would like to see is in the hiring. Lots of comments have been made about the speed with which the commercial sector can identify high-quality cyber personnel and hire them. But the slowness of, especially on the civilian side of—

Mrs. DAVIS. The personnel system, yes.

Dr. SCHMIDT. Yes. So I think that is one way that the DOD could improve to be able to be more competitive with the commercial sector.

Mr. DELFINO. Congresswoman, I think there are two answers for this question. As we talked about the people, I think we can talk a little bit about the technology now. As a vendor, the regulatory burden of doing business with the government is very high. It is unlike any other market that we play in. As a relatively young 16-year-old software company who does hundreds of millions of dollars in the public sector, including the DOD, for the most part we don't hold direct contracts, but instead provide products and service through resellers and distributors who do hold contracts with the government. This is a fairly substantial impediment to younger technology companies who may have offerings that could substantially help the DOD.

And the second to that is funding. It is difficult for the customer to find ways to acquire innovative technology following today's acquisition appropriations process. An IT cycle is 24 months. However, once a product is in development, there is often a delay in getting it into the government.

So the private sector has the ability here to, you know, in all reality stay 2 to 3 years ahead of the government if they choose to do so.

Mrs. DAVIS. Yeah. Thank you.

The CHAIRMAN. Thank you.

Chairman Wilson.

Mr. WILSON. Thank you, Mr. Chairman. And thank you and Ranking Member Smith for arranging for cyber week this week. We have the hearing today. Tomorrow again at 10. Tomorrow afternoon. It has been a real honor for me to work with Congressman Langevin as the ranking member on Emerging Threats. This really has been a bipartisan effort to address the issues we have. And we also have an extraordinary professional staff, as I referenced in a 1-minute yesterday.

For Mr. Bejtlich and Mr. Wallace, you have touched on this, and that is in regard to attribution. What is our capability? And then how much attribution is necessary or can be achieved to provide for a response such as sanctions against individuals, businesses, military units, maybe a nation?

Mr. BEJTLICH. Sir, briefly, the way I like to think about attribution is that the government, the military, the IC have capabilities that exceed the private sector when you think about the source of attacks. They have the legal authority and they have the national

technical means to get very close, and to even infiltrate, who the adversaries are.

The private sector, on the other hand, our expertise tends to lie at the other end. We are with the victims. We are helping the victims. We are seeing what the adversary is doing within the victim companies.

So when you put those two things together, we have a very good picture of what is happening. Now, the government doesn't necessarily tell us what they know. We tend to tell the government what we know by working through our customers.

So you put those two things together, and when you add in the idea that attribution is ultimately a political question, it is not necessarily a technical question, you have very strong attribution capabilities now.

Mr. WALLACE. I would just add to what Mr. Bejtlich said to say that the level of attribution you require depends what you want to achieve. And since it is a political decision, it depends what political acts you want to take. One of the most, I think, important things going forward is going to be able to take other nations with you in your actions, and that is going to require increasingly greater level of attribution in helping those countries understand the reasons that you are taking the actions that you are.

Mr. WILSON. And, Mr. Bejtlich, I would look forward to receiving information about the hacker in Kunming. Ironically, my dad was stationed in Kunming with the 14th Air Force in World War II and always he was so grateful for the opportunity to protect the people of China from the attacks. And so it is somewhat ironic now that there would be attacks from there potentially. There should be a reminder of the relationships that we have had.

And, Dr. Schmidt and Mr. Delfino, something that I hope can be done, the technologies change so quickly, and, to me, there needs to be a real effort and advice, and I know Secretary Carter has been working on this, but what can be done to promote public-private partnership?

Mr. DELFINO. I do feel that there is a pretty strong public-private partnership not only within the DOD, but throughout other U.S. Government agencies as well. I think some of the risk that we manage today is due to the scale of legacy implementations that we have and the amount of effort it would take to moving something like the JIE.

So I believe that, through reading through the documents and the initiatives and the goals of the JIE, there has been a good amount of consultation between the DOD and the private sector as well, and I do believe it is reflected in that document as well. So I commend the DOD for that.

Dr. SCHMIDT. The topic of a public-private partnership is a bit outside my area of expertise, but I will point you to the recent information-sharing proposals that have come forward in various bills. And I think that the sentiment there is that while information sharing between the government and the public sector is possibly a beneficial arrangement, it is not necessarily a panacea. And there is testimony from my colleague Martin Libicki that explains that it depends upon the actions of the threat actors. And if they can get inside the time with which we can share information from

the government to the corporate sector, it may not have the benefits that it is designed to have.

Mr. WILSON. And we look forward to all of you in providing information to us on how we can expedite a public-private partnership.

And a final for Mr. Bejtlich. Is there any way for us to respond back where there has been a hacking?

Mr. BEJTlich. Yes, sir. I think the notion of hack-back is something that is often asked of the private sector. I believe the state should retain a monopoly on force and retain that as a potential state function.

Mr. WILSON. Thank you very much.

The CHAIRMAN. Interesting question we probably have more questions to ask about.

Mr. Cooper.

Mr. COOPER. [Audio malfunction in hearing room.]

The CHAIRMAN. Mr. Johnson.

Mr. JOHNSON. Thank you, Mr. Chairman.

Mr. Bejtlich, do you believe it is worthwhile for the Federal Government to initiate negotiations with other nations when it comes to avoiding cyber conflict, cyber war?

Mr. BEJTlich. Yes, sir, I do. I think the example with China is a good one, where it was difficult for us to establish a norm saying that we should not steal each other's secrets in order to provide them to the private sectors of each country. Now that we have actually established that as a norm publicly, I think it is a good idea to take to other locations.

Mr. JOHNSON. Does anyone disagree with that on the panel or have anything to add to it?

Mr. WALLACE. I would just add that we already have norms, even laws against countries going to war with each other. What we actually need to seek to do is find ways to avoid that happening by accident. So we shouldn't throw out all of the experience or the international law that exist. We need to better understand how we integrate cyber into those frameworks.

Mr. JOHNSON. Is there a role for an international organization such as the U.N. [United Nations] in this new cyber arena where there needs to be clear rules established for conduct of folks internationally, both private and—or both government and nongovernment entities?

Mr. WALLACE. So the United Nations is already engaged in this area. They have a group of government experts who have been meeting over a number of years to sit around a table and negotiate, at least agree the norms of behavior that should exist. They have essentially over a number of years agreed that what happens—that international law should apply.

What I think possibly we have to do now is move into other fora where blocking countries, those countries who make life difficult, are not present, and to move together to try to implement some other norms a little bit more aggressively.

Mr. JOHNSON. Do you see a future where the U.S. goes it alone and seeks to be the world superpower, dominant, in control, and kind of a go-it-alone attitude about the cyber arena when it comes to just dominance and enforcement? I know I am not being eloquent with my question, but I think you might know what I mean.

Mr. BEJTLICH. Sir, I do know what you mean. And it is interesting, this is one of the fears some other countries have. The Chinese, for example, are very aware that much of the hardware—not necessarily the hardware, they make the hardware over there. But we make the software. We have the innovative companies. We have the protocols. We have the core of the stakeholder agreements that run the Internet, and they are looking for a way to better integrate and in some ways exert their own control over that.

So I do believe this idea of more inclusion for all the affected parties matters. It was different years ago when we were the dominant force in terms of users. Now we are rapidly becoming less and less compared to the hundreds of millions of people elsewhere.

Dr. SCHMIDT. If I could just add a few points. You will notice that the DOD strategy points to the need to build partnerships with international players on this line, not necessarily to dominate, as you asked originally, but to build security and safety for all the players.

Mr. JOHNSON. Thank you. And I will yield back my time.

Mr. WILSON [presiding]. Thank you, Mr. Johnson.

We now proceed to Congressman Wittman of Virginia.

Mr. WITTMAN. Thank you, Mr. Chairman. I thank the members of the panel for joining us today.

Several of you had mentioned earlier concerning members of the military, and number one, their abilities, but also what we would do to make sure they have the proper education within cybersecurity. And let me get your perspective on several different levels.

How important is it for us as a nation to train our future military leaders, specifically in the realm of cybersecurity? Not just a cursory introduction, but an in-depth educational experience at our service academies, through our ROTC programs. And, secondly, how important is it for us to make sure that every enlistee in every branch of the services gets some level of training and education within cybersecurity?

It seems to me that having a higher level of expertise throughout the service ranks would be a great advantage to us, especially with the eyes and ears and the skills that they might have to be on the lookout, but also to think intuitively and creatively about not only how to prevent cyberattacks, but look at how we can be better defensively, but also things we could do on the offensive side.

So I would like to get your perspective on that on both of those levels.

Mr. BEJTLICH. Yes, sir. I agree with your idea of—over the entire spectrum of someone's career. My wife was an operations officer at a basic training squadron in the Air Force. I know the schedule is tight, but that 18-year-old enlisted person is the way into the force many times. So don't put them through some boring set of slides where they just look and sort of stare at it. Put them through a little exercise, where they are in front of the computer; they get that email, they go to that Web site, whatever it is so that they know what it looks like.

I also think it needs to be taught at the academies, as you mentioned, at the mid-level and senior-level schools, but this is also, I think, where the cyber force comes in. We need people who can defend themselves. We also need those people who think about this

in that domain, and that is the way that they approach this problem.

And that's what I think—I firmly believe in 20 years we are going to look back and wonder, how did we not have such a capability?

Mr. WALLACE. I think it is essential that we have better cyber education, as I have already argued. I think there are two separate aspects to that education; cybersecurity and awareness of the vulnerabilities at a personal level, and at a institutional level, also an awareness of cyber operations. I disagree with Mr. Bejtlich. I think imbedding an understanding of cyber operations within the current services may be a more sensible way forward.

But I think we both agree that having a better appreciation of how wars will be fought in the cyber context is going to be essential for military leaders, and that has to start right at the beginning of their military education.

Mr. WITTMAN. Mr. Delfino.

Mr. DELFINO. So I think certainly, those people in positions in the military leading people whose primary objective is cyber efforts need to have very deep cyber expertise themselves, not just be, you know, a more generalized leader.

I think as it relates to the more general or the broader enlisted service men and women, they certainly need to be trained on best practices to prevent themselves from becoming a point of compromise and entry into the DOD infrastructure. And also need to learn what happens if in mid-mission a system that they are using or dependent upon for that mission is breached and is no longer there, how would they deal with that from a circumstances perspective as well? So, I would not attempt to turn every enlisted member into a cybersecurity expert, is likely infeasible.

Mr. WITTMAN. Dr. Schmidt.

Dr. SCHMIDT. I think research shows that it requires a depth of expertise in the cyber workforce, but also in the leaders of the cyber workforce. I think there is a tendency to think that managers can just have a broader understanding, but our research indicates that that is not the case. And to keep up with the technology trends, the evolving threats, the leaders also have to be deep in their expertise, and so I would support a deeper cyber education for military leadership, DOD leadership. And that has to be refreshed over time due to the dynamic nature of the cyberspace.

Mr. WITTMAN. One additional question. How important is pay to retain those experts across the spectrum of needed expertise, but also in the different areas of the service branches both on the civilian side and the uniform service side?

Mr. BEJTLICH. So pay is important, but it is not everything. In 2001, when I got out of the Air Force, I didn't get out because I wasn't making enough money. I got out because there was no career path. I would have gladly stayed. I would have even been more inclined to stay if I knew I could go to the private sector for a couple of years, go back into the military. You can do things in the military you can't do anywhere else, so it is quite a retention bonus.

Mr. WITTMAN. Any other thoughts? Mr. Delfino.

Mr. DELFINO. Just as in my written testimony as well, I think pay is a component of it, and I do believe that the government can be competitive there and the DOD as well. I believe it is also a training investment, an ongoing training and development investment to keep people sharp. The ability for them to get industry accreditations that they can use post their service either in the military or as a civilian in the Department of Defense as well. And a career path I also highlighted in my written testimony is very, very important for these individuals as well.

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

Mr. WILSON. And thank you, Chairman Wittman.

We now proceed with Mr. O'Rourke of Texas.

Mr. O'ROURKE. Thank you, Mr. Chairman.

Mr. Bejtlich, you said earlier that perhaps the most important question for us to answer is the amount of loss that we are willing to tolerate. And I like that, because if we had a chief information security officer that is a level to which we hold that person accountable and responsible for. If we are trying to communicate consequences to our adversaries, we can say, you know, this is the level, whereas now it is a little ambiguous.

How would you advise us to proceed in answering that question? What are the factors that you take into account? And do you have an answer to it?

Mr. BEJTLICH. Sir, I do. I would start by taking a look at the metrics we use to assess whether we are winning or not. The way I like to describe it is this, we spend a lot of time measuring the height of our players, how fast they run the 40, where they went to college, and we don't figure out what the score of the football game is. So we are doing a lot of input metrics; we are not taking a look at what the outcome of the game is. So the outcome of the game in cyberspace for me would be how many intrusions are occurring over a certain period of time? What were the consequences of those intrusions? How quickly did we find out that it had happened?

Just, you know, to give you an example, the front page of USA Today the other day said, Energy hacked 159 times in 4 years. This is a step in the right direction? But this doesn't say, "How bad was it?" "What actually happened?" I could look at this and say, "This isn't actually too bad." So we need to turn more towards metrics like this and less from we have certain numbers of systems patched and so forth.

Mr. O'ROURKE. And in terms of communicating that level of tolerance to an adversary, is that something that is made explicit, if you do this, these will be the consequences, both cyber and perhaps physically militarily for crossing this red line or this threshold?

Mr. BEJTLICH. I think there needs to be something like that. And I know Secretary Panetta at one point said that in, I think it was an October 2011 speech he gave, where he said if there is significant consequence to the power sector, financial—he laid out certain categories that they would be met by a response, not just as Mr. Wallace mentioned in cyberspace, but outside of cyberspace. So, we have to keep delivering that message. And when something significant happens, like OPM, we should take a response. We just can't say, well, this is something that we would have done as well.

In the Cold War when a spy ring was uncovered, we didn't say, well, the Soviet Union spies. We kicked them out, we might kick out the ambassador. So there can be consequences that signal our disapproval of that action.

Mr. O'ROURKE. Mr. Wallace, I really enjoyed your analogy comparing what we are doing today to the development of military aviation prior to World War II. And you seem to suggest that in the United States we were rewarding risk-taking, and through that attracting the best and brightest, and ensuring that they have career advancement connected to that risk-taking and that advancement of military aviation.

Can you give me a specific example of what we are not doing in the U.S. if we are, in fact, not doing that today in cyber? And perhaps to ask it in a positive way, what we could be doing, what we should be doing, and as specific as you can get?

Mr. WALLACE. So I would say in defense of the commanders of today that back in the 1920s, U.S. Navy had a very clear sense of who its adversary was likely to be and worked around that. But I think they were more imaginative and they did take steps that are not being taken today.

One very specific example is Admiral King. When he was a captain, quite advanced in his career, was taken and trained as an aviator so that he had the qualifications, because Congress had passed laws to say you needed to be an aviator in order to command an aircraft carrier. And therefore as some other senior officers got that qualification.

So they understood not only the actual process of flying an aircraft, but also had an appreciation of the tactics that would be required and the organization, putting the carrier at the center of the battle fleet rather than the battleship, that would be necessary to go on and prevail in the operations that followed in the 1920s.

Mr. O'ROURKE. What is the analogy to cyber? What are we not doing? Who is not getting the training? Is it senior commanders within the Department of Defense?

Mr. WALLACE. Rather than treating cyber operators off to the side, as the sort of techies, it is integrating cyber into military operations and having those people who understand cyber operations as part of the group of people who go on to command full-spectrum operations.

Mr. O'ROURKE. Thank you.

Mr. Chairman, I yield back.

Mr. WILSON. Thank you, Mr. O'Rourke.

We now proceed to Congressman Rich Nugent of Florida.

Mr. NUGENT. Thank you, Mr. Chairman. And I appreciate this panel.

Now I sit on ETC, and we hear, obviously in classified settings, issues as it relates to how we are going to do certain things. But I guess what strikes me though is, you know, what we can tolerate or what we are willing to tolerate. And I don't know that we have a whole lot of discussion on that. And so then when you start saying, okay, what are the consequences to your actions? And there really—that is pretty undefined also.

Do you think to date that we have been, I guess, succinct enough to talk about consequences to actions, particularly as it relates to

just China and what's gone on? We heard about the fact that we indicted five. You know, prior law enforcement, that would be a problem for me if we indicted them and they were residents of the United States where we had extradition abilities, but, I mean, that sounds good, but what other consequences have we imposed when we clearly know who the actors were?

And it is just not China. I mean, there is other actors out there: Russia, Iran, and others, and North Korea. What other sanctions have we imposed to date? Can anyone speak to that?

Mr. BEJTLICH. Sir, my own personal experience, I have been working intrusions by Romanian hackers, Russian, Chinese, criminal nation-states for—in the private sector, post-military for 13, 14 years now, and we are only now seeing consequences. Now, there has been a decent amount of law enforcement work that has been done, but in terms of going after, say, businesses that have benefitted from the theft of commercial information, we still haven't done that.

Mr. NUGENT. Please.

Mr. WALLACE. I would say that I think we have to remember that the issue is bounded. There is a level which, I think, adversaries know they shouldn't go. There is also the fact that law enforcement does take care of cyber intrusions in many more friendly countries around the world, say, for a smaller area.

And in relation to the PLA five, the colonels that were indicted. I think there is a debate as to whether that was the right tactical action. But I think one thing that could be said in favor of it, is that at least it began the process of preventing a negative norm, the idea that countries can act with impunity and not have any kind of acknowledgement that that is unacceptable behavior.

Mr. DELFINO. I will just add to that, that there may be times where we want to respond offensively cyberly, while maintaining confidentiality and not take a responsibility for those responses as well in order to not divulge our level of sophistication and our responses as well.

Mr. NUGENT. I agree.

Dr. SCHMIDT. And to build on that, one of the things that the DOD strategy has set out as a goal is to be able to respond when a contingency comes up and the desire is to implement an offensive cyber capability. I think one of the critical areas where we need to be working is ensuring that commanders know how those offensive cyber capabilities will perform if they are called upon to be used.

And we could be doing more in that area to characterize their performance and ensure that they do not have unintended effects.

Mr. NUGENT. I agree. One statement was made, I think Mr. Delfino, you were talking about, is our reliance on technology within the military is so high, whether it is ground troops, obviously, air troops, whether it is naval engagements. Are we doing enough in regards to challenging those members of the military to say, okay, this system crashed or is down because of a cyberattack? Are we doing enough in any of your estimation to, I guess, work around that particular issue? Are we doing enough within the military?

Mr. DELFINO. I think it is a good question. I think there is three attributes of what we do, you know, people and process, and the third one being technology. Are we doing enough? Are we giving

these people the technology they need fast enough and the funding that they need fast enough to make the changes that they need to prevent those or recover from them when they happen, I think is a good question, and is part of why we see this JIE initiative. Because I think they have noted that the legacy approaches that they have been taking have increased complexity substantially. So it is a big challenge for them.

Mr. BEJTICH. Just briefly, sir. I agree with your sense of that. We need to war-game with major systems not being available, GPS [Global Positioning System], and so forth, and see how people respond.

Mr. NUGENT. Mr. Chairman, my time has expired. I yield back. Thank you.

Mr. WILSON. Thank you. Thank you, Sheriff Nugent.

We now proceed to Mr. Aguilar of Texas—of California. And I want to thank—Congressman Aguilar actually came early, so this is good.

Mr. AGUILAR. And stuck around late. Thanks, Mr. Chairman. I appreciate it.

Mr. Bejtlich, you mentioned in your testimony, I think the fifth point, how the administration should develop asymmetric capabilities to target the core interests of the bad actors, and you mentioned one. And building off of what Mr. Nugent mentioned, you talked about the censorship network in China. What other asymmetric examples do you believe are available not only with respect to China but other actors like Russia?

Mr. BEJTICH. You know, it is interesting you mention Russia. No one really talks about the degree of instrumentation they have in their country. One of the interesting aspects of the Russia-China dynamic is that they have agreed to work on Internet security mechanisms. And what that really means is Internet control mechanisms, dissident suppression mechanisms.

So, they are developing software to make it easier for them to target their dissidents both inside and outside the country. So, just as easily as we could go after the Great Firewall, we could look for vulnerabilities in that software that those two countries are developing and figure out ways to exploit it, degrade it, potentially even render it inoperable.

Clearly, control is important to those regimes, and I gave one example to the Great Firewall in China, but there is similar activities you could do elsewhere.

Mr. AGUILAR. And what other countries? What other examples?

Mr. BEJTICH. Well, if we are going to talk, the big ones we worry about, North Korea, their core interest is in the stability of the regime and keeping out outside influence. So we could work on ways to better—right now there are people sending DVDs [digital versatile discs] into North Korea using balloons. We could potentially get SATCOM [satellite communications] or Mesh Network equipment into that country, make it easier for people to get information real time rather than having to wait for a balloon to make it across the border.

Mr. AGUILAR. Thank you.

Mr. Bejtlich, you also mentioned in the discussion about collaboration and public-private partnerships other potential to embed

folks, my words, not yours, in private companies. Can you talk a little bit about structurally how that would work? How you would have liked that to work in 2000, 2001 when you were still in the military service?

Mr. BEJTICH. It is a great question. So, I was an incident responder in the Air Force. I would have loved to have been able to go to Mandiant for 2 years. It didn't exist at the time, but let's say now you go to Mandiant, you do incident response for 2 years inside private companies; you learn how to use the tools that the private sector uses, you learn what private sector networks look like; you learn what the adversary does in those environments.

At the same time the private sector company learns from your capabilities. You have to respect the classification and all that, but that dynamic is what makes for a powerful capability. And then, so after the 2-year period I would go back into the military and I would continue down my career path. And perhaps even go back at a later time, maybe as an executive, maybe at another time going and teach. While we do have a great educational system in this country, there is many people who think that security is encryption. We need more people who spend time in the trenches teaching that next generation of security professional.

Mr. AGUILAR. Thank you very much.

I yield back, Mr. Chairman.

Mr. WILSON. And thank you, Mr. Aguilar.

We now proceed to Congresswoman Jackie Walorski, of Indiana.

Mrs. WALORSKI. Thank you, Mr. Chairman. And thank you, panel, for being here. I appreciate it.

I represent Indiana, where I know you mentioned this has been talked about before—the National Guard is looking at those new cyber force teams, and we are thrilled that Indiana is going to be involved in our National Guard.

But I just had a question. I think, Mr. Wallace, you had talked about the possibility of over-relying on DOD and defending the Nation from cyber threat. In August, I was on a trip to Czech Republic. And in Czech Republic, the subject of Estonia came up in the 2007 giant cyberattack in Estonia, and they developed the cyber defense league. And I know that our DOD worked some with that. Any of you can answer this question. But I looked at that and some of the things the little tiny nation was able to do, which really is building an alliance very quickly. Is that a model that our country looks at? I know we are somewhat a part of it, but can you speak to the significance or the success Estonia has had as opposed where to where we are? Is that something we should look at more seriously?

Mr. BEJTICH. I do. I think Estonia has the advantage of being small, 1.7 million people; they can be nimble. They had a threat that was very visible to the entire country.

In this country, I think we could have, in addition to the cyber force, we could have something like a cyber corps. Now I know there's one that exists, but it's not really very popular. I'm thinking more of like a Peace Corps model where you get some training; you go to a one-month boot camp, and then you can deploy within either our country or perhaps even overseas, and you can be that cybersecurity expert for that small- to medium-size business.

I would love to hire a person like that who had just been through a 2-year program out in the field. There is a big difference between book learning and learning out on the job. So there is, I think, many ways to involve people, not just in the military, but through government service to improve their cybersecurity.

Mrs. WALORSKI. Mr. Wallace.

Mr. WALLACE. I would completely agree with that. I think Estonia is a particular case, its history, and its small size, the fact that people tend to know each other. But I do think there is something in the fact that the cyber defense league is both a military and a nonmilitary organization.

And I think the idea to be involved in national security you have to be in uniform is something that in the age of sort of cyber capabilities we need to move away from. And something that, as Richard suggests, takes a more imaginative approach to how we manage some of the threats we face is definitely something that could well be explored.

Mrs. WALORSKI. And is there a benefit in displaying some offensive cyber capabilities in some way that we do possess as a nation, or—it seems that, of all the hearings that I have sat in, we always hear the lack, the holes, things we could be doing better. Are there things that we actually do right now that are kind of like the kingpins that hold us together to be able to at least get the information that we have without going into anything that we classified.

Is there a benefit in kind of letting the world know that we are not just playing catch-up; there are things to at least get out there in the cyber world that we are doing or something like that?

Mr. DELFINO. I think there is a benefit to doing the offense, I don't know if there is a benefit to displaying it.

Mrs. WALORSKI. So how would we do the offense? And what would we do internally? When would we do that? Because it seems like that isn't happening.

Mr. DELFINO. Right. And I think, you know, there are things that we don't know that we assume that the U.S. does because we are not taking responsibility for that. Right? Stuxnet and the Iranian nuclear reactor would be a good example of that. Right? And I don't know that we could claim credit for that, nor do I think we should.

Mrs. WALORSKI. Right.

Mr. DELFINO. However, leaving the enemy guessing about was that a response for something I did may be a very good tactic offensively.

Mrs. WALORSKI. Yeah. Mr. Wallace.

Mr. WALLACE. I also think that we shouldn't necessarily think of offensive cyber operations purely in the context of a stand-alone covert operation, which are probably outside the realms of the DOD's title 10 mission.

But, actually, there may well be opportunities within a warfighting context where you can save lives, but the lives of U.S. personnel and indeed, civilians and perhaps even enemy by using capabilities, putting down an air defense capability that you couldn't do with kinetic weapons. And I think it is difficult to demonstrate, but over time could prove extremely important.

Mrs. WALORSKI. I appreciate it.

Thank you, Mr. Chairman. I yield back.

Mr. WILSON. And thank you, Mrs. Walorski.
And we now proceed to Mr. Ashford of Nebraska.
Mr. ASHFORD. Thank you, Mr. Chairman.

This has been extremely interesting to me, this conversation, and we have learned a lot.

Of course, it was dramatized in the movie at Bletchley Park when Ultra was just developed during World War II. And one of the parts—and you have talked about this a little bit, but maybe we can talk about it just a little more, but the idea, the cultural, sort of obstacles that we saw in Bletchley Park at the beginning, before the code was broken and during that whole process—I realize it is a while ago, but Mr. Wallace talked about prior to World War II and the developments in Britain, and you've talked about the cultural thing. But I am really intrigued by it.

I know in Omaha, where I am from, Omaha, Nebraska, there are many young private sector tech startup companies that do—have had some, maybe some history with these kinds of matters. And you have talked about it, but how do we break down those cultural barriers? Could you go through that once again? We encourage people to work on this. They can go back to the private sector, I get that. Would you say these cultural barriers are significant? Are they being worked on? What is your vision timeframe-wise to kind of break down some of these boundaries and obstacles to integration, getting the best people working on these issues? Maybe just—

Mr. BEJTLICH. Certainly. So my observation has been in certain parts there is more supply than demand. So the Army has gone through a very successful exercise, putting out a call, for people within the service now who want to go into cyber. And they have gotten many applicants. Things are going well.

The question is, where are they going to be in 2 years or 4 years. You have already seen the attempt to build a Cyber Mission Force and other parts at Cyber Command. They are still struggling to fill those spots. I do think when you are looking at military personnel, ultimately, how are they rewarded? How are they viewed compared to their peers?

You know, in the Air Force, you know, the pilots were the top. You are not going to get a cyber commander of the Air Force. You are not maybe even going to get an intel commander of the Air Force. You could probably get an airlift commander of the Air Force, but you are not going to get some of these other people. So I think if you want to be able to keep and retain the best for the longest period of time, you are going to eventually have to break them off and have them be their own.

Now, that doesn't mean no cyber or any other forces. I think tactical cyber supporting physical missions should remain with the other services, cyber, it is in everybody's lives. But I think that at the end of the day, strategic cyber is probably going to have to be its own service with its own culture and its own ethos.

Mr. ASHFORD. Mr. Wallace.

Mr. WALLACE. Practice, war-gaming, going through the motions, working between the services, bringing in the private sector to go through scenarios that reflect events that may happen in the future is, to my mind, the best way of identifying the problems, get-

ting people of different cultures to understand ahead of the point where they have to do it for real where the other people are coming from.

And to the point that Congressman O'Rourke made about analogies, one of the real triumphs of the interwar years was practicing and trying things out before having to do them for real and developing new concepts off the back of that. And I think that is going to be important in this area too.

Mr. ASHFORD. Thank you.

Mr. DELFINO. I would just add, in the context of public-private partnership in this area, you could make a private sector rotation, job rotation, a condition of promotion to the Senior Executive Service as well as part of this.

Mr. ASHFORD. Thank you. Dr. Schmidt.

Dr. SCHMIDT. With regard to rotating between public and private, I think one of the key problems that DOD faces is retaining the highly skilled folks around the 6- to 8-year mark. And that is, in fact, what Mr. Bejtlich was talking about, about this time that he was starting to get interested in the commercial sector.

So if there can be something done to help retain those folks either through incentives to stay in or other opportunities to rotate to the commercial sector, that could help solve one of DOD's primary problems.

Mr. ASHFORD. All right. Thank you very much. I think we have talked a lot about that with the NDAA [National Defense Authorization Act] this year, to try to think about how do we retain. And in this area it is a significant challenge. Thank you very much.

And I yield back. Thanks, Mr. Chairman.

The CHAIRMAN [presiding]. Thank you.

Ms. Gabbard.

Ms. GABBARD. Thank you very much, Mr. Chairman.

You know, the issue that you are bringing up of how to just completely change the way we think about how we bring in the best talent to deal with these cybersecurity challenges and thinking outside the traditional concept of well, it has to be in uniform if you are dealing with the Department of Defense I think is really at the crux of all this, to make sure that we are on the cutting edge of this constantly changing and dynamic area.

I am interested to hear your thoughts on Secretary Carter's implementing this initiative to work closer with Silicon Valley, what you see, maybe the pros and cons of that, how we can benefit, or maybe what some of the barriers are to the DOD being able to really get the best of what that policy, I think, hopes to accomplish.

Mr. BEJTLICH. Just two quick points, ma'am. I would like to endorse Mr. Delfino's earlier comments about the difficulty of small companies doing business with DOD. And on a related point, when we are operating under continuing resolutions, it is tough to get new programs going. And so that has been a challenge for the private sector for the last several years.

Mr. WALLACE. I would just add that I think it is absolutely essential that the DOD has access to the best technology available, but I also think it is important to recognize that working with Silicon Valley it is not a silver bullet. There are good reasons why Silicon Valley companies who depend on international markets for

their entire business model, they're not necessarily going to roll over and work with the DOD in the way that DOD might necessarily want. So, I think it is important, but it is not the silver bullet, nor do I think that DOD thinks it is.

Dr. SCHMIDT. I would just like to point out that I think things like pursuing personnel that have STEM [science, technology, engineering, and mathematics] degrees in electrical engineering, computer science, information technology, would go a lot further than a couple of small initiatives associated with Silicon Valley.

Mr. DELFINO. I would have to agree extensively with Dr. Schmidt here. I don't think this problem should be that complicated. I think if you are pursuing a career in cybersecurity or information technology as a long-term investment, I am sure many of us would be thrilled to hire folks who worked in cybersecurity and U.S. Department of Defense or other U.S. intelligent agencies as well, and they would be rewarded greatly.

So, I think this is about keeping the pipeline of talent coming in. I am sure that we don't want the DOD to become the training ground for information technology in cybersecurity across America. However, our ability to attract that young talent going into university and coming out of university, particularly from those acclaimed universities, is something that the DOD can successfully do.

Ms. GABBARD. Thank you. And forgive me for coming in late if you have already addressed this. If you could briefly state the major cybersecurity breaches that we have seen across the Federal Government, really within the last several months, would you say those are primarily attributed to a lack of technical capability, or is this a larger policy issue?

Mr. DELFINO. I don't think this is so much as a policy issue, and I don't think they differentiate dramatically from those that we are seeing in the private sector either. There are common exploits that the attackers are using across both public and private sector as well as military and classified networks as well. I have addressed a list to some extent in my written statement. We continue to see this, and until we change the technology that we are using, we are going to continue to see this.

The private sector exploits of Target and Home Depot and JPMorgan Chase that we saw were 3 years ago from companies that are extremely sophisticated, wildly intelligent, and have massive technology budgets. And there are some fundamental, foundational network architecture problems that are allowing these attacks to continue to happen. And until we change the way we build and construct these and automate these infrastructures as well, both from putting security in to defending once we see a cyber-attack, we would likely continue to see these issues.

Ms. GABBARD. Do you see those changes being implemented in the private sector?

Mr. DELFINO. They are in the acceleration stage of being implemented in the private sector. So these are things that are not new now. People get the reason why. They have tried traditional methods. I would point you back to General Keith Alexander's comment, former director of National Security Agency: "I look at the DOD architectures today, and defending them is really hard. We have 15,000 enclaves, each individually managed."

People are starting to realize that physical separation, you know, can get you security to a point, but as you start to scale it becomes unmanageable, operationally infeasible, and over time becomes so complex you actually may get reduced security from it.

Ms. GABBARD. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you. Mr. Wilson.

Mr. WILSON. Thank you, Mr. Chairman. And again, thank each of you for your input today.

Mr. Bejtlich, with your military background, what is the role that DOD should have in protecting the critical infrastructure from cyberattack or intellectual property from cyber espionage?

Mr. BEJTlich. Thank you for the question, sir. As I mentioned in my written testimony, I think it is difficult to have the DOD directly involved at the customer end of this problem. For the most part, these sectors don't want troops stationed nearby. They don't want government sensors on their networks. So I feel that that is the realm of the private sector and those entities themselves, which can be guided, perhaps, through better incentives and regulation.

But I think that as far as DOD is concerned, I would put pressure on those adversaries twofold. One, you want to know what they are up to so you can interdict their activities. And, two, you want to introduce some friction into their activities so they don't have free rein against their targets. And then when they do see something coming down the pike, you have got to warn those targets that this is about to happen and work with them to try to prevent that breach from occurring.

Mr. WILSON. And, then specifically, I am concerned about the electrical grid. And so what would be the DOD role to protect the electrical grid for the people of the United States?

Mr. BEJTlich. I would identify which foreign actors are considering trying to take down the power grid. I would target their activities. And when I see them trying to or planning to do something like that, I would hit them preemptively.

This is one of the cases where it would be worth the gain-loss in the intel equation to disrupt their activities, and potentially lose a source rather than sit back and have to recover from a power grid failure.

Mr. WILSON. And for anyone who would like to answer, I am really concerned about DOD protecting its networks and mission systems from attack. Has this adequately been provided?

Dr. SCHMIDT. I think that's yet to be determined. Certainly, the risk management approach that they have put in place is an excellent step in the right direction, but it all comes down to the implementation of that framework. I think identifying the vulnerabilities and more critically their tie to missions is what it is all going to come down to.

I think the strategy doesn't fully describe how they will implement that objective, and I would like to hear more about the implementations, specifically, for missions systems and how it relates to critical DOD missions.

Mr. WILSON. And I am particularly concerned about the systems relative to air defense. Would anybody comment on that, or missile defense?

Mr. BEJTlich. Sir, it is interesting you bring that up. Air defense is one of the physical systems that has an attack, a cyberattack, associated with it. Apparently, there has been—the Israeli Air Force did something to Syria at some point in the last 5 years. We don't really have any unclassified corroboration of this. I am not saying I have classified corroboration; I am just saying this is what I have read. So it is potentially a system that has seen a physical effect due to cyber.

Mr. WILSON. And I have a great concern about the capabilities of DPRK [Democratic People's Republic of Korea], North Korea, and its capability of intercontinental ballistic missiles with an inability on our part to protect the American people. Is that a legitimate concern?

Mr. DELFINO. Sir, I think, you know, there are elements of the DOD and the government, specifically STRATCOM [Strategic Command] is doing very well at this, the DISA [Defense Information Systems Agency] milCloud is doing very well at this, and specifically, the Missile Defense Agency is doing well in implementing automation and cloud-based technologies and the appropriate security technologies to protect that infrastructure from DPRK or other nation-state actors as well.

Mr. WILSON. And a challenge it's developing, is the capability of mobile missiles being developed by—such an extraordinary challenge and threat to us. And so, again, I want to thank you for being here, and we all look forward to your input to protect the American people.

I yield.

The CHAIRMAN. Thank you.

Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. And I also would be remiss in not acknowledging and thanking Chairman Wilson for his leadership on this issue as well. It has been a real pleasure working with him as the chairman, me as the ranking member, he as the chairman of the Emerging Threats and Capabilities Subcommittee. He has really done a deep dive on this, and I appreciate his leadership, so thank you, to both chairmen.

So if I could just ask a couple last questions that I had. Given your disparate backgrounds, if each of you could see the DOD CIO successfully and fully implement just one policy, what would it be?

Mr. Bejtlich, want to start with you and go down the line.

Mr. BEJTlich. Sir, I think you win the toughest question award for the hearing.

I would like to see a strategy that is based—first of all, a strategy, that is based on recognizing that adversaries will get into the network, that the goal should be to minimize what they can do, and that you achieve that by seeing them as quickly as possible and containing them.

And then being a beacon for the rest of the government. This is one of the few areas, I think, where—not one of the few areas, but this is an area where DOD does a pretty good job already. So taking that expertise and leveraging it and teaching the rest of the government would be a great achievement.

Mr. LANGEVIN. Thank you.

Mr. WALLACE. I am afraid that question probably takes me beyond my level of expertise, but I certainly don't disagree with what Mr. Bejtlich said, that making sure that the DOD's expertise is leveraged by the rest of government and learning the lessons. DOD is not perfect, but taking those lessons and leveraging them across government I think is an opportunity that should be taken.

Mr. DELFINO. Congressman, I will simply respond by saying, I think if the DOD only did one thing, we would have a much bigger problem. I think the first thing they need to do is recognize that this is a multifaceted, complex problem which requires multiple serial strategies being put in place simultaneously to address.

So if they only do one thing or there is really not one thing that is more important than the many things that need to be done here. And I do think that the Joint Information Environment is a good step in the right direction, caveating the successful execution and implementation of that technology.

Dr. SCHMIDT. I think DOD has recently issued policies that are aimed at securing the cyber acquisition chain. So looking at major weapons systems acquisition and thinking about how to properly do that such that they are defensible in the future. I think that that has been a good step. What I think could also be needed is looking at legacy weapon systems, the ones that are already fielded and that where the cyber acquisition policies won't come into play as effectively, what can DOD do to make sure that those legacy weapon systems are cyber secure.

Mr. LANGEVIN. Thank you. And if I could, Dr. Schmidt. I find your testimony regarding deliberate planning for cyber operations very interesting.

What should we do today to enable the kind of deep analytic work you refer to?

Dr. SCHMIDT. So I am referring to a deliberate planning for cyber operations in terms of getting those offensive capabilities ready to be used in case they are called upon to do so. And so commanders need to have the confidence in those kind of capabilities that they have in conventional weapons. So we have had decades upon decades of experimentation and tests and very rigorous test designs, data collection, and analysis efforts that have led to, on the conventional side, deep physics models and an understanding of how those weapons are going to perform when they are called upon to be used.

I think we need exactly the same thing on the offensive cyber side, and that is going to require an investment in designing those kinds of tests to explore how they're going to be used, what the operational conditions will be in those settings, and especially to ensure that the offensive cyber capabilities don't have unintended effects. Because only then will commanders have the confidence that is required to deploy those capabilities to contribute to the deterrence that we desire.

Mr. LANGEVIN. Is DOD paying enough attention right now to that? In the sense that war-gaming these types of things out and so they fully understand the capabilities they have at their disposal and how to use them?

Dr. SCHMIDT. I think it is a growing area of concentration. I definitely think more could be done to make sure that we characterize the capabilities.

Mr. LANGEVIN. Okay. Thank you.

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

The CHAIRMAN. Thank you.

I want to, I guess in some ways, follow through on some of that. I don't think we talked too much about supply chain, and yet there are very few things DOD buys these days that don't have some component, either the hardware or the software, that comes from other places. And, you know, mostly when we talk about cyber we think about networks and going through the Internet to have effects somewhere else.

But do any of you all have suggestions on this supply chain issue where there may be corrupted, tampered hardware or software that makes it into important systems that create vulnerabilities for us? And probably, my guess is, there is no way we can be assured of finding it all. So what do we do?

Mr. DELFINO. Thank you, Mr. Chairman.

This is why we have to move to a model where there is no longer a trusted element inside of the infrastructure as well. Whether it was maliciously tampered with by a private entity or a foreign government or somebody within the United States itself or it is just, many of these devices that we are finding today that are being inputted into the network have software in them that has known vulnerabilities, right? And I don't know that the DOD has the ability to test every single device that comes into its infrastructure itself.

And this moves to the model where we have to have—there is no longer a people outside the perimeter are untrusted and people within the perimeter are trusted. Everybody has to be treated as an untrusted entity so that at the time that that device or piece of software tries to propagate malware or a virus or spyware within the environment, it can be detected automatically and shut down and defended against.

Mr. BEJTLICH. Sir, just briefly. I come at it from a slightly different angle. I would come at it from the counterintelligence perspective. Best way to find out if the adversary has ways into your system is to be inside theirs and notice, hey, these guys are getting into our systems, or they have a plan to do so, or they have a team that is standing up to do that activity. That could be potentially another way to find out what's happening.

The CHAIRMAN. Both Mr. Bejtlich and Mr. Wallace say that the Federal Government, the military, should not defend private infrastructure, although Mr. Bejtlich says, well, we ought to create some friction, you know, don't let them have it too easy, which is kind of an interesting subplot.

So if I am a major company—if I own a bunch of refineries in the Houston ship channel and a bunch of bombers come my way, I know what I expect the United States Air Force to do to protect me. A bunch of packets come against those same refineries from somewhere, I may or may not have the ability to get the attribution on that. I take your point on attribution. So the Federal Government is not going to defend me, so I am left on my own. And

my options, then, are to sit there and take it or have, if I am sophisticated enough, some sort of retribution on my own, which leads to all sorts of problems.

Is that really a good scenario? And if other nation-states or terrorist organizations or Russian mafia know that we won't defend these companies, doesn't that open it up and they know how far to go and to take advantage of it? So explain to me why that is a preferable way of doing things.

Mr. WALLACE. Can I just clarify my answer?

The CHAIRMAN. Yes, of course. I obviously summarized in great generalities.

Mr. WALLACE. So, in extremis, I absolutely believe that it is the role of the military to defend the United States against attacks of a serious consequence. What I think is important, however, is to avoid the military becoming the first place that the private sector turns to when it feels under threat.

There is a number of other places that they can go, firstly, others in the private sector to improve not only their capabilities to defend themselves, but also that resilience when they do get attacked, the deterrence by denial, if you like.

Secondly, I think it is not necessarily the case—that in this area that you need to be wearing a uniform and having gone through military training to be—to be a Federal Government employee supporting the private sector. And so, it doesn't need to be the case that the military has to be the place even within the Federal Government that the private sector would turn to when it feels it needs to.

And so my point is not necessarily that the military shouldn't defend the private sector in certainly, particularly, in a warfighting environment where the homeland is under threat as a result of what the military is potentially doing overseas, there needs to be cooperation. But I do think that if the military becomes the first place everyone turns to, that is going to be a burden which the military cannot bear in the long term.

Mr. BEJTICH. Sir, if I could address it as well. I agree with what Mr. Wallace said, but I also would like to mention two things. One, would the government have been effective as it was with, say, OPM? Maybe not. Who knows.

So, the second issue is one of time. I think there is a perception, and you probably even hear it from some of the witnesses, not here, thankfully, but sometimes witnesses wearing uniforms, where they talk about attacks at the speed of light or attacks at network speed. And it is this idea that there is this magic that is going to happen in a couple of seconds the whole world will explode. My own research has shown that many times it is taking days, weeks, even months from when an adversary first gets into a target to when they have their effect. So if at any point during that time, generally, it is a couple of weeks to a month, you are able to interrupt their activities, you win and they lose.

So that gives time for, if the private sector entity hasn't dealt with it, you know, within the first week or whatever it is, the government can step in and say, hey look, you guys have a problem; you need to deal with this before they accomplish their mission. So I think there can be ways to have the government help without

having say, government security equipment inside private sector organizations.

Mr. DELFINO. I think we need to be careful to say, should the DOD defend these American companies versus should they secure them and monitor them actively to see if they are under attack. I think if the DOD saw an active attack on a private sector U.S. entity by a foreign nation-state backer and had the ability to, they may stop it.

But I do think it is a fair question to say, is it the responsibility of the DOD to respond on behalf of that private entity because of that, right? So if a warfighter was to show up and bomb a U.S. refinery, the DOD may defend that in the physical world and maybe should potentially do that in the virtual world as well. But I think we need to be careful not to take the responsibility off these private entities to secure and monitor their own infrastructure as well.

Dr. SCHMIDT. And the strategy also provides for DOD's role in protecting critical U.S. interests of significant consequence, which would include loss of life and significant damage to property, although your—

The CHAIRMAN. It says that, but I don't really know what they mean by that, which is part of why I was wanting to see what you all thought.

I had one more, and I forgot what it was.

Oh. Most of what we talk about is others stealing information. According to press reports, the Iranians actually destroyed computers with Aramco that had some consequence for the Saudi oil production. Do you all regard it as inevitable that at some point it won't just be stealing information, but there will be destruction of data or hardware, that there is inevitable escalation to these things with potentially more serious consequences on loss of life and so forth?

Mr. BEJTICH. Sir, that is an excellent question. I do see that. Also not just wholesale destruction. It could be subtle corruption such that we can't trust what we are dealing with, which in some ways I would be more worried about, because at least if it is destroyed, I know, okay, I have to restore it from backups and such. But even the restoration part. There was a great talk recently by a young lady who was involved in the incident response at Saudi Aramco. They basically went to Japan, South Korea, and bought every laptop, hard drive, computer that they could find in order to bring that refinery back. That is not something you are going to be able to do over and over again.

Mr. WALLACE. I think over time, anything can happen. And definitely capabilities do exist to conduct destructive attacks. But I think we should be careful in expecting motivations of actors in cyberspace to be fundamentally different from actors outside of cyberspace. And there are significant reasons why adversaries would not want to conduct an out-of-the-blue attack.

Where I think it is of more concern potentially, is inside a war-fighting scenario where the United States is engaged overseas, it would be certainly an asymmetric option open to the adversary that was not available in years past to make an attack on the U.S. homeland. And understanding that dynamic I think is going to be

important and probably more likely to be something that the DOD should consider than a bolt from the blue attack.

As DNI [Director of National Intelligence] Clapper I think, said recently, data manipulation may be a more likely and worrying scenario than something destructive like Saudi Aramco.

The CHAIRMAN. Okay. I am sorry. Did you have something you wanted to add?

Dr. SCHMIDT. I was just going to mention that data manipulation is certainly being demonstrated in the academic sector. There are several studies that show that manipulating small bits of information, for example, in GPS signals can cause unexpected reactions when the data is processed within the computer and the GPS receiver, and it is something that DOD will have to take very seriously.

The CHAIRMAN. It is a great point, and I guess kind of related to that, what, I think may be more likely is the sort of plausible deniability, it is not really us, you know, this is just happening on its own. We are seeing that in warfare in general to cause confusion and uncertainty to slow the response. And I agree if it is active warfare, then all holds are barred, but even to put pressure on our economy doing things with the banking system that you can't quite figure out why it is slowing down, et cetera, is a huge challenge.

We could talk much of the day about the challenges we face. I really appreciate you all being here, and I think you have helped set up a number of the issues that we will address to the deputy secretary and Admiral Rogers tomorrow.

And so thank you for your testimony. With that, the hearing stands adjourned.

[Whereupon, at 11:58 a.m., the committee was adjourned.]

A P P E N D I X

SEPTEMBER 29, 2015

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

SEPTEMBER 29, 2015

Statement for the Record

Richard Bejtlich

Chief Security Strategist

FireEye, Inc.

Before the

U.S. House of Representatives

Committee on Armed Services

Outside Perspectives

on the

Department of Defense Cyber Strategy

September 29, 2015

Chairman Thornberry, Ranking Member Smith, members of the Committee, thank you for the opportunity to testify. I am Richard Bejtlich, Chief Security Strategist at FireEye. I am also a nonresident senior fellow at the Brookings Institution, and I am pursuing a PhD in war studies from King's College London. I began my security career as a military intelligence officer in 1997 at the Air Force Information Warfare Center.

My employer, FireEye, provides software to stop digital intruders, with 3,400 customers in 67 countries, including 250 of the Fortune 500. Our Mandiant consulting service, known for its 2013 report on Chinese PLA Unit 61398, helps companies identify and recover from intrusions. In 2014, we conducted hundreds of investigations in 13 countries.

As a private sector defense strategist and as a former military officer, I assess the new DoD cyber strategy as a transition document. Previous strategies emphasized DoD's role as protecting DoD networks from attack. The current document restates this role, and adds a new albeit limited mission: "defend the US homeland and vital interests from disruptive or destructive cyber attacks of significant consequence." Stepping outside the Beltway mentality, it might be natural to ask "what about OPM?" or even "what about Sony?" For these reasons I believe DoD's strategy is a step in the right direction, but one that needs to be augmented by additional measures.

Before listing my recommendations, I would like to briefly discuss four relevant topics: private sector security capabilities, attribution, hack-back, and acquisition.

In 2013 Mandiant published its APT1 report, exposing a Shanghai-based military unit that had attacked over 140 companies in a seven year period. Since then many other security companies and private research organizations have released reports describing a variety of hacking teams. Some organizations, like the Atlantic Council, have exposed the operations of Russian soldiers in Ukraine, again using open source media, tools, and techniques. These reports are part of a revolution in private sector intelligence.

Government and private parties each bring unique perspectives and capabilities to the attribution problem. Government analysts, using national technical means, can apply advanced signals, imagery, and human collection capabilities to hard targets, getting closer to the source of malicious activity.

Private companies and organizations can work more closely with the victims of malicious activity, often in ways not available to government agencies. Combining these two perspectives produces a more complete picture of adversary activity and enables more effective countermeasures.

The revolution in private sector capabilities has shattered the myth that attribution in cyber space is impossible. I recommend reading *Attributing Cyber Attacks* by Dr. Thomas Rid and Ben Buchanan to better appreciate the integration of political context with technical details. It is true that some national and criminal hacking teams are improving their operational security as a means to frustrate attribution work. However, the explosion in social media across the developed and developing world means the people behind the hacking continue to show more of their actions and personalities in public forums. Just last week two security companies combined forces to use social media and other online sources to expose a member of a military hacking unit in Kunming, China. I assess that improved information sharing will also drive forward the attribution capabilities of public and private teams.

Attribution matters because it contributes to verification and stability. Last week Presidents Obama and Xi stated that “neither country’s government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.” The success of this agreement rests on the ability of each party to identify malicious activity emanating from the other, and positively attribute it to the government-controlled and sanctioned teams operating on behalf of each party. This requires high levels of attribution on both sides, in the public and private spheres. Government attribution capabilities are important because they inform the quiet, inside advisors to decision makers. Private attribution matters because they are the louder, outside voice to the media and citizenry.

Consider the difference between “high” and “low” attribution capabilities. I define high attribution capabilities as the integration of technical and political analysis to detect and identify digital adversaries. Those lacking this skill are said to have “low” attribution capabilities. For an example of “high-high” attribution, imagine the US and Russia. For “high-low,” imagine the US and China. For “low-low,” imagine Vietnam and China. One way to measure attribution capabilities is to watch for private sector companies in the country of interest who can release high-quality security reports. In the US, we have

Mandiant and others. In Russia, Kaspersky. In China, Qihoo-360 is a rising star. None come to mind for Vietnam, for example.

When two opponents each possess high attribution capabilities, it becomes difficult for a malicious third party to run a “false flag” operation, trying to trick the opponents into escalating a conflict. Two parties with high attribution capabilities are also able to determine if attacks emanating from certain locations are the work of the nation state, or are the result of a third party hijacking computers in the hosting country.

When either one, or both, opponents possess low attribution capabilities, it is a less stable situation. This could be a problem with the agreement between China and the US. Private and public teams in the US can perform high levels of attribution on Chinese activity. Private and public teams in China do not share the same capabilities at present. China could therefore suspect that the US is behind certain hacks, although such activity could be caused by Russia or other actors. This is one reason to welcome the rise of private or nongovernment security companies in China, who may improve the country’s attribution capabilities.

Despite my praise for the private sector, I do not advocate giving non-government parties the authority to conduct offensive operations, also known as “hack back.” I worry that private sector offensive operations could invoke an escalatory spiral, for which the national government would be ultimately responsible. Also, despite my faith in private sector attribution, offensive operations require target knowledge that could exceed the capabilities of many private parties. Therefore, I recommend that the state retain the monopoly on violence by reserving for itself the right to hack-back.

The last hot topic is acquisition. DoD and other government agencies should adopt acquisition practices that seek best-value solutions, rather than lowest-cost providers. Too often we see DoD and other groups acquire products or solutions that meet narrow technical specifications, and succeed in frustrating only the most basic attacks. Congruent with Secretary Carter’s efforts to involve Silicon Valley and foster innovation, it is crucial that DoD be open to testing and acquiring capabilities that can stand up to the worst adversaries. Furthermore, DoD must integrate a secure software development lifecycle approach to the weapons and systems it procures. Processes such as the Building Security In Maturity Model (BSIMM) should be incorporated such that DoD weapons and systems are as resilient as possible

to digital attack. Red teaming should also be applied at multiple stages of the development lifecycle, not simply when capabilities are in the field. It is much cheaper and more effective to discover and fix flaws when weapons and systems are being designed and built, rather than trying to remediate vulnerabilities near or on the battlefield.

Beyond the specifics of the DoD strategy, I would like to offer five recommendations to improve the nation's digital security. Three involve DoD and two involve the administration and other agencies.

First, I recommend DoD and the Intelligence Community modify the nature of offensive digital operations against national adversaries. According to open source intelligence tradecraft and stories published in open media, US government offensive digital activities currently focus on traditional espionage targets. These operations fulfill collection requirements such that US government decision makers can execute their duties, based on accurate and actionable intelligence. Foreign intelligence services also conduct these operations. However, foreign intelligence services, military units, and other teams also attack private sector companies, civil society organizations, and even individuals. US offensive digital capabilities should therefore be ordered to directly target the foreign teams that are attacking private US entities.

By putting pressure on these foreign teams, US victims would receive some relief from the relentless waves of foreign hacking campaigns. By "pressure" I mean low-level activities that introduce friction and uncertainty into the minds and processes of foreign hackers. For example, US offensive teams could quietly corrupt tools and infrastructure used by foreign teams against domestic targets. They could periodically crash foreign computers used to hack US targets, or degrade bandwidth used to transport malicious traffic. The idea is to introduce obstacles into foreign hacking operations, such that they are working uphill when trying to attack US victims.

Second, the DoD, the IC, and partners should consider indirect ways to help protect US private sector and associated targets. If government actors learn that private entities are being targeted by a foreign adversary, they should be more willing to warn of the attack before it happens. For the past eight years or so, the FBI and other intelligence organizations have provided valuable third party notification services. These are post-breach warnings to private US entities after the FBI or other agency determines that a foreign actor has stolen data from the private US entity.

In situations where the US is unwilling to directly disrupt foreign hacking activity, DoD or the IC should inform private entities about pending hacks. This concept, like the previous idea of putting direct pressure on foreign hacking teams, involves sensitive equities. Intelligence and cyber operators do not want to risk jeopardizing sources and methods by notifying victims of impending attacks. However, the government must do more than simply notify the private sector when they fall prey to advanced foreign hacking operations.

Third, Congress should sponsor studies, by a mix of government and private sector researchers, to determine the costs and benefits of creating an independent new digital military service, or Cyber Force. As a former captain who performed the computer network defense mission in the Air Force, I am pleased to see the existing military services improving the career paths and opportunities for today's troops. After speaking at an Army Cyber Institute event last week, I watched two Army captains explain how they would apply cyber tactics and tools to accomplish a simulated physical combat mission. Unfortunately, I was reminded of the challenges facing these young officers when an audience member warned the pair that their non-cyber colleagues might "think they were playing warrior," and that their makeshift technical solution might appear to be a toy.

These cultural barriers are real and inherent in each military service's ethos. My tentative proposal is that so-called tactical cyber missions, where digital tools support a physical mission, should remain with the existing services. Strategic cyber missions, where digital tools are the primary focus, should become the realm of a new Cyber Force. Each service thinks differently, and rewards different skills and accomplishments, and my sense is that we need a Cyber Force to recruit and retain the nation's most promising digital warriors. The Cyber Force could also pioneer the more flexible, agile, information-age acquisition, promotion, placement, and leadership practices advocated by Defense Secretary Carter and Under Secretary Carson.

Fourth, I recommend the President appoint a US Chief Information Security Officer (US CISO). The Executive Branch has a Chief Information Officer (CIO) and a Chief Technology Officer (CTO), but not a CISO. This is similar to the situation at many businesses prior to a breach, although the Federal government has repeatedly found itself in a post-breach situation. The US CISO should share the same rank as Megan Smith, current US CTO, who is an Assistant to the President. The US CISO should have

operational control of a Federal Computer Incident Response Team, or FedCIRT. The FedCIRT would be a joint, interagency team composed of representatives from across the government. The purpose of the FedCIRT would be to hunt for intruders in non-intelligence, non-defense networks, and conduct joint incident response and recovery operations with the affected departments and agencies. The US CISO should pay particular attention to government cloud infrastructure.

Fifth, the administration should develop the capability to take asymmetric actions that target adversary core interests, but in a way that leverages our strengths against their weaknesses. For example, in the case of China, the so-called Great Firewall is an important target. The Chinese government uses its Great Firewall to censor content it considers to be a threat to the Chinese Communist's Party control of the country. The New York Times published a story in early August describing how the administration was considering taking steps to undermine the Great Firewall as a response to the Office of Personnel Management breach. This action offers excellent flexibility that can be calibrated according to the signal and effects the government wishes to achieve. At the low end, the US could fund research to enable bypassing the Great Firewall. At the high end, the government could sponsor covert activity to enable censorship-free Internet access via satellite or mesh communications. Such actions would impose cost on the Chinese government in a way they would recognize and perceive as a reflection of core US interests, should the agreement between Presidents Obama and Xi not pan out. The ability to inflict asymmetric cost on adversaries is a core element of deterrence, which I believe plays a role in the digital arena.

I look forward to your questions.

Richard Bejtlich
Chief Security Strategist at
FireEye

Richard Bejtlich is Chief Security Strategist at FireEye, and was Mandiant's Chief Security Officer when FireEye acquired Mandiant in 2013. He is a nonresident senior fellow at the Brookings Institution and an advisor to Threat Stack, Sqrrl, and Critical Stack. He is pursuing a Master/Doctor of Philosophy in War Studies at King's College London. He was previously Director of Incident Response for General Electric, where he built and led the 40-member GE Computer Incident Response Team (GE-CIRT). Richard began his digital security career as a military intelligence officer in 1997 at the Air Force Computer Emergency Response Team (AFCERT), Air Force Information Warfare Center (AFIWC), and Air Intelligence Agency (AIA). Richard is a graduate of Harvard University and the United States Air Force Academy. His fourth book is "The Practice of Network Security Monitoring" (nostarch.com/nsm). He also writes for his blog (taosecurity.blogspot.com) and Twitter ([@taosecurity](https://twitter.com/taosecurity)).

**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 114th 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: Richard Bejtlich

Capacity in which appearing: (check one)

- Individual
 Representative

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

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:

2015 FireEye has multiple contracts with numerous US Federal government agencies and foreign governments for cybersecurity products and services which are relevant to the subject matter of this hearing. Pursuant to these agreements, FireEye is subject to non-disclosure provisions.

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

2014

FireEye has multiple contracts with numerous US Federal government agencies and foreign governments for cybersecurity products and services which are relevant to the subject matter of this hearing. Pursuant to these agreements, FireEye is subject to non-disclosure provisions.

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

2013

FireEye has multiple contracts with numerous US Federal government agencies and foreign governments for cybersecurity products and services which are relevant to the subject matter of this hearing. Pursuant to these agreements, FireEye is subject to non-disclosure provisions.

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:

2015

FireEye has multiple contracts with numerous US Federal government agencies and foreign governments for cybersecurity products and services which are relevant to the subject matter of this hearing. Pursuant to these agreements, FireEye is subject to non-disclosure provisions.

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

2014 FireEye has multiple contracts with numerous US Federal government agencies and foreign governments for cybersecurity products and services which are relevant to the subject matter of this hearing. Pursuant to these agreements, FireEye is subject to non-disclosure provisions.

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

2013 FireEye has multiple contracts with numerous US Federal government agencies and foreign governments for cybersecurity products and services which are relevant to the subject matter of this hearing. Pursuant to these agreements, FireEye is subject to non-disclosure provisions.

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

Testimony to the House Armed Services Committee

Ian Wallace

Senior Fellow, International Security Program & Co-Director of the Cybersecurity Initiative,

New America

September 29, 2015

Chairman Thornberry, Ranking Member Smith, distinguished committee members, thank you for inviting me to testify on the Department of Defense (DOD)'s Strategy for Cyberspace. Let me first make clear, that I am testifying in a personal capacity and my comments should not be taken to reflect those of my former employer, the British Ministry of Defence.

OVERVIEW

The DOD's Strategy for Cyberspace, published in April this year, is a welcome and necessary update to the DOD's 2011 Strategy for Operating in Cyberspace, which was at the time an important and timely document. But the public conversation has evolved and it was, for example, becoming increasingly untenable for DOD's extant strategy not to acknowledge the United States' offensive cyber capability.

Cyber capabilities will undoubtedly play a major role in the future of war, and international relations more generally. The strategy demonstrates the considerable progress that the DOD has made in responding to the new challenges. That said, this still remains an emerging area in which no one yet has all the answers. Therefore, this exercise in opening up the DOD's thinking for public discussion should be welcomed and encouraged.

Nevertheless, despite the progress that the Department of Defense (DOD) has made, the Strategy is not perfect. There is more work to do particularly in establishing the exact role that the DOD should play in defending against cyber threat to the rest of Government and the private sector; and in preparing for the future operating environment. Against that background, and in the spirit of constructive criticism, I offer the following concerns that I believe warrant further inquiry.

WHAT IS THE ROLE OF THE DOD IN CYBERSPACE, ESPECIALLY IN 'DEFENDING THE NATION'?

My first major concern relates to second of DOD's self-appointed missions: 'conducting cyber operations to counter an imminent or on-going attack against the U.S. homeland or U.S. interests in cyberspace'¹. It is relatively easy to infer what 'success' would look like when it comes to defending DOD's own networks: even if it is not possible to keep all attackers off those systems, early identification of intrusions and the removal of the intruder will be as important for DOD as for any major organization. Equally, ultimate success in terms of supporting the warfighter will be success on the battlefield. I have some concerns about the depth and breadth DOD thinking on how to achieve that goal (see below), but not in the goal itself.

On the other hand, the DOD's exact responsibilities for defending of the U.S. homeland are less clear. The Strategy talks of being 'prepared to defend the U.S. homeland and U.S. vital interests from disruptive and destructive attacks of significant consequence.' And the Strategy goes on to emphasize that use of DOD assets should be the exception. It is clear that this has been a topic of discussion within

¹ The DOD Cyber Strategy, U.S. Department of Defense, April 2015, p5

the Administration. It might also and reasonably be argued that it would be unhelpful to give potential attackers too clear an indication on when DOD would engage in a public document.

Nevertheless, particularly in the absence of a wider, up-to-date U.S. Government Strategy for Cyberspace (a major problem for the Strategy, although not the fault of DOD itself) how much the U.S. Government will depend on the DOD remains unclear. In an effort to provide reassurance that such DOD intervention in support of the private sector will be rare, Principal Cyber Advisor to the Defense Secretary Eric Rosenbach told the emerging threats and capabilities subcommittee of the Senate Armed Service Committee in April this year that the DOD would only act in the 'top 2%, the most serious'² of cases. In doing so, however, he only raised more questions about what that really means.

Why does this matter? For two reasons: first because a fundamental aspect of good strategy is prioritization. There are opportunity costs related to the establishment of the National Mission Force: in relation of other DOD cyber missions, in relation to other non-cyber defense capabilities, and in relation to wider non-defense priorities. And second because the way in which this mission is described in the Strategy assumes that the DOD's main role in defending the U.S. homeland from cyberattack is likely to be in cyberspace.

It is not that this mission is wrong in itself. As the Strategy points out, the DOD is 'in concert with other agencies ... is responsible for defending the U.S. homeland and U.S. interests from attack'³. It therefore needs to ensure that it has the capability to fulfill that responsibility. It might even be argued that the very existence of the National Mission Force represents part of a credible deterrence strategy. My concern, however, is that bureaucracies have a tendency to 'do their thing', and military bureaucracies doubly so. Once the National Mission Force become established and has proven its worth, it will be tempting for others to take it for granted. My contention is that the aim should for the use of DOD capabilities to 'defend the nation' from bad actors in cyberspace to be seen as a failure of wider government policy, not the normal course of events.

Neither should we think of the National Cyber Force as the Department of Defense's only contribution to defending the U.S. homeland or vital interests from cyberattack. As set out in the 2011 International Cyberspace Strategy⁴, the United States reserves the right respond 'by all necessary means' to a cyberattack, i.e., including outside of cyberspace. I believe that there is a good case to be made that one of the reasons that we have not so far experienced a very serious level of disruption or destruction is that potential attackers understand that to do so would risk a significant military response. To put it another way, there are plenty of people in the world who would like to do harm to the United States, and the tools to cause trouble in cyberspace are widely proliferated. However, given the prospect of a military response, even nation state actors have kept their actions at a level below which would justify a military response. Such threats are not easy to manage, but they do not have to be the responsibility of the DOD. Such logic does not negate the need for a National Cyber Force. It could have a major role to play when deterrence has already failed – for example with a war, or when states feel their existence is under threat and they have nothing to lose.

² Eric Rosenbach, Principal Cyber Advisor to the Defense Secretary, Hearing to Receive Testimony on Military Cyber Programs and Posture in Review of the Defense Authorization Request for Fiscal Year 2016 And the Future Year Defense Program, emerging threats and capabilities subcommittee of the Senate Armed Services Committee, April 14, 2015

³ The DOD Cyber Strategy, U.S. Department of Defense, April 2015, p2

⁴ The International Strategy for Cyberspace, The White House, May 2011, p14

Put simply, therefore, the 'defend the nation' mission will require careful and ongoing oversight to ensure that it remains properly sized to meet the need, as well as ensuring that others in Government and in the private sector do not come to depend too heavily on DOD for activities that do not need to be carried out by uniformed personnel.

DOES THE STRATEGY PROPERLY PREPARE THE DOD FOR THE FUTURE?

Another important question to ask of the Strategy is: Does it prepare DOD for the future challenges the military will face? One of the opportunity costs of an over-emphasis on the 'defend the nation' mission is that we risk crowding out time and resources for imaginative thinking about the ways in which cyber capabilities will affect the way in which future wars will be fought, and what that means for the United States military. My second concern is that the Strategy focuses so closely on preparing the Department for the challenges of today that it risks overlooking the need to prepare for the cyber challenges of tomorrow.

While the Strategy document acknowledges the need to respond to the actions of potential rivals, it is less clear from the document that the DOD has fully internalized the effect of the globalization of information technologies and its implications. Yet good strategy is inherently competitive and potential rivals are not standing still.

Other initiatives, such as the so-called 'Third Offset Strategy', show that there are some within the Pentagon who appreciate the future challenge. However, it is less clear from reading the Strategy for Cyberspace how much impact that thinking is having on cyber policy. This is not the place for a full discussion of the future operating environment, but there are several trends that will affect the way in which the United States uses its cyber capabilities that the Committee might like to ensure that the DOD is addressing.

- a. Technology – While the importance of research and development is highlighted in the Strategy, there is relatively little focus on the extent to which the technology, to date an important contributor to the United States' competitive advantage on the battlefield, will increasingly become a leveler in global affairs. This is particular true with regards to cyber capabilities for which the barriers to entry are relatively low (especially as much of the technology is commercially sourced) and through which other, increasingly networked, military capabilities can be attacked. The United States may well find plenty of ways to maintain a technological edge, but the DOD's plans to do that with regard to cyber capabilities will be key to future military success (even if not part of the unclassified Strategy document).
- b. Organization – while the Strategy does go into detail in the way in which the DOD has reorganized itself to deliver the three cyber missions, we should not expect that this will be the last reorganization. And nor should it be. Historically militaries who adapt successfully to new technology often do so by changing the way in which they organize to fight. While the Strategy focuses on the Cyber Mission Force, the true organizational challenge will be in adapting the wider U.S. Forces. This does not mean that every Service member needs to become a 'cyber warrior', but existing organizational constructs are unlikely to be perfectly suited to the changed operating environment. The implications of that will be difficult for the institutions affected, but to ignore that is to risk a future adversary exploiting that unwillingness to adapt.

Just as in the Interwar years, the U.S. Navy applied some of their finest minds to classroom wargames and live exercises in order to find the right organizational concepts to incorporate

carrier aviation (leading to the replacement of the battleship with the aircraft carrier at the center of the fleet), operational experimentation will be key. This time, however, to be truly successful, such experimentation will need to be properly Joint, and – given the strength of Service interests – that means actively supported from the top of the Department. The Committee should not expect that DOD will already have all the answers on future force structures, but it should expect senior DOD leaders to display a commitment to explore new ideas.

- c. Allies – One of the best features of the Strategy is its recognition of the importance of Allies to the United States' future military edge. As potential rivals develop increasingly sophisticated technology, it will be the United States' ability to build and maintain alliances that will ensure its military edge. While the proposed actions in the Strategy make sense, the challenges in refreshing old alliances (and building new ones to take advantage of the new opportunities offered by cyberspace) and the time and work required should not be under-estimated. The support and the encouragement of the Committee to such efforts will be important, especially as such efforts are likely to take time and considerable commitment.
- d. People - The biggest opportunity for the United States military to maintain its competitive advantage in the 21st century will likely come from the quality of its people. While the Strategy acknowledges the importance of the workforce by making its development part of its first Strategic Goal, the Strategy tends to focus on the Cyber Mission Force. While that is understandable in the short to medium term, it raises questions about the capacity of the wider force to appreciate the constraints and opportunities created by the new technology and therefore the ability of the force to fully adapt. While it is understandable that DOD does not yet have all the answers to what the arrival of cyber capabilities into the battlespace means for the wider force, the Committee should expect them to be asking these questions.

To summarize: the Strategy offers a good road map to achieving the DOD's own sense of what it needs to do to achieve its responsibilities in cyberspace. I believe that that the analysis is largely correct, but that the DOD will require outside support in several key areas, most obviously in calibrating the military's role in defending the United States from cyberattack and ensuring that the significant near term challenges do not crowd out thinking about how to remain competitive on the wars of the future.

Ian Wallace
Senior Fellow, International
Security Program

Ian Wallace is a Senior Fellow in the International Security Program, and also Co-Director of New America's Cybersecurity Initiative. His research is mainly focused on the international security and military dimensions of cybersecurity policy. He is also a member of the 'Future of War' project.

Ian joined New America from the Brookings Institution where he spent two years in the Foreign Policy Program as a Visiting Fellow for Cybersecurity. He was previously a senior official at the British Ministry of Defence (MOD). From 2009-2013 Wallace was as the British Embassy, Washington's defense policy and nuclear counselor. There he helped develop new UK/US mil/mil cyber link at both the operational and policy levels. Before joining the embassy he was a fellow at the Weatherhead Center at Harvard University where his research included working on the military implications of cyber capabilities.

During his UK MOD career, he combined strategy and planning positions with operational postings to Pristina (2001-2002), Basra (2005) and Baghdad (2007-2008). He also served as the head of policy at the UK's operational HQ (2002-2003). His Whitehall appointments included Deputy Director of Capability, Resource and Scrutiny and Assistant Director of Defence Resources (with day-to-day responsibility for the UK MOD's overall resource planning process). From 2000-2001 he was the Assistant Private Secretary to the UK Defence Secretary.

Wallace has a degree in ancient and modern history from Christ Church, Oxford 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 114th 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: Peter Ian Wallace

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:

2015

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

2014

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

2013

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:

2015

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

2014

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

2013

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
Salary, allowances, reimbursements (month of Jan only)	British Government	7193.74	Salary, allowances, reimbursements (month of Jan only)

Statement for the Record

Dominick (Dom) Delfino, Vice President

World Wide Systems Engineering

Networking and Security Business

VMware, Inc.

Before the

U.S. House of Representatives

Committee on Armed Services

Outside Perspectives on the Department of Defense
Cyber Strategy

September 29th, 2015

Chairman Thornberry, Ranking Member Smith, and Members of the Committee, thank you for the opportunity to testify today. I am Dominick (Dom) Delfino, Vice President of World Wide Networking and Systems Engineering at VMware.

My employer, VMware, is the fourth largest software company in the world, with 2014 revenues of over \$6 billion and over 18,000 employees. VMware has more than 500,000 customers and 75,000 partners, including 100 percent of the Fortune 100. VMware serves all sectors of the U.S. Government; including the Department of Defense, the Civilian agencies, and the Intelligence Community, as well as state and local governments. The company is headquartered in Silicon Valley with 140 offices throughout the world.

VMware is a leading provider of software defined solutions that make data centers across the globe operate more efficiently and securely and allows both government and commercial organizations to respond to dynamic business needs in on premise datacenters, in the cloud, and on personal computers and mobile devices. VMware is providing enhanced security to commercial and government customers globally through its pioneering role in redefining how we build and secure networks, data centers, and computers and devices.

Thank you for the opportunity to provide our views on the DoD Cyber Strategy released in April.

Cyber-Attacks: Clear and Persistent Threat to the U.S. Government

The U.S. Government depends on a vast cyber world of interconnected IT networks, data centers, the Cloud, mobile platforms, and other assets. Individual agencies rely on this cyber infrastructure to perform almost every mission critical function within their purview – from national defense and natural disaster response to postal services and the constitutionally mandated Census. In many cases, multiple agencies are interconnected at various operational levels to facilitate the sharing of business systems information and/or to provide interagency support to meet common mission objectives. The widespread adoption and use of cyber-systems has reaped immeasurable benefits for the country through increased government responsiveness, agency effectiveness, worker productivity, and a host of other economic efficiencies and returns.

Because we require cyber infrastructure to perform the modern day functions of Government, sophisticated and aggressive cyber-attacks perpetrated by criminal entities and foreign government agencies represent a clear and persistent national security threat to the U.S. Government. Recent well-publicized cyber-attacks have targeted the Department of Defense, the Office of Personnel Management, U.S. Postal Service, the U.S. State Department, the Internal Revenue Service, and other agencies.

Department of Defense Cyber Strategy

Goal 1: Build and maintain ready forces and capabilities to conduct cyberspace operations

We believe that DoD's Cyber Strategy is a good first step towards improving the Department's cyber posture. Providing our cyber warriors with the skills to fight this battle is a challenge due to the variety of constant changing threats and missions they face on a daily basis. VMware believes that this challenge, while seemingly daunting, can be managed with a few industry proven practices.

1. Realistic and robust simulated cyber-training environments are needed to effectively develop and test the skills of cyber warriors. Current methods for engaging the cyber threat require high levels of training on complex tools and costly security products. By applying currently available technology, these environments can be built on demand, represent the evolving threat and not require an army of support contractors. Once in place, these cyber classrooms can provide on-demand training to warfighters globally. VMware has worked with organizations such as the Ft. Gordon Cyber Leadership School to pilot these capabilities with promising results.
2. We recommend DoD leverage currently available automation technologies and simplify the cyber detection and course of action. By creating push-button responses that can be just as rapidly undone, the Department can empower today's cyber warriors with the ability to stop threats immediately, even temporarily, without having to wait for a complex change process. Today, to deploy a cyber countermeasure such as blocking an attacker or modifying a firewall, is a timely and complex process that takes hours or days when every minute counts. With automation, more on demand, yet immediate countermeasures can be deployed to stop specific threats. With this capability DoD can

rapidly expand the courses of action without requiring years of training on complex tools. This would allow current experts to automate simple countermeasures and reserve the best and brightest cyber warriors for the most significant threats such as searching for unexploited vulnerabilities and developing tactics and techniques.

The United States Government, the DoD as well as other agencies responsible for dealing with cyber security should undertake a significant initiative to attract, recruit, retain and train a talent pool to stay at the forefront of cyber security knowledge. Attracting the right talent is one of the most challenging aspects of creating a cyber defense operation. My suggestions are as follows:

1. The U.S. Government, and more specifically the DoD, has the ability to be competitive with private sector for cyber talent, but it must be creative in its tactics and use programs like the special hiring authority which allows agencies to pay a higher wage for experienced personnel with specialized skills. The DoD should consider a blend of civilian employees, military personnel and contractors.
2. Require ongoing training and development and create a cyber promotion path. Technologies and threats evolve rapidly today. Cyber skills need to be updated frequently in order to stay ahead of our adversaries. Personnel in this field should receive one full week of training per quarter inclusive of Industry and DoD relevant certifications and accreditations. DoD may also want to consider creating a career track so that cyber warriors have promotion paths to command level responsibility.

Goal 2: Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions

As the Department is implementing its new Cyber Strategy, security should not only focus on the perimeter because the current approach it is not working. We know the threat landscape is constantly evolving; as soon as one vulnerability is mitigated, another threat vector arises. The attackers deal strictly with software that is being written, updated, and refined on a daily basis and this fact puts our agencies at a tactical disadvantage on a daily basis. Government networks that rely on a traditional hardware-based perimeter security strategy will never be able to keep pace with an ever-changing software-defined world.

The recent attacks on our Government have had one thing in common: the attacker, once inside the network perimeter security, was able to move freely around the victim's network. It is clear to our nation and to those who perpetrate these attacks that the way in which we protect our national cyber infrastructure, and the way in which most federal entities and agencies design and deploy cyber security systems is ineffective.

Too much trust is placed on perimeter-based security and human responses to secure networks. As history has shown, this approach leaves our nation vulnerable and at a significant disadvantage. Hackers were able to penetrate perimeter network security systems and subsequently gain access to systems where they were free to access and steal sensitive data over a period of several months. Hackers typically use this attack methodology because traditional perimeter-centric security systems are structurally designed to be “doors” to the network. These doors serve to allow authorized users access to networked systems and to prevent unauthorized users from getting inside a network. However, the structure of perimeter-based security makes it the single point of failure (a single perimeter: firewall + additional security systems like intrusion prevention or advanced attack detection) that must be breached in order to enter the data center network. Once the intruder has penetrated perimeter security there is no simple means to stop malicious activity within the data center without extreme disruption to the agency’s mission. In many cases, the response from agencies and network security vendors is to add more security technology to the perimeter; this response ignores the structural insufficiencies.

Mitigating the economic, political, and social damage to our nation from these types of cyber-attacks demands that we change the way we build, operate, and secure our Government’s mission critical IT infrastructure.

VMware submits three salient points for consideration:

- 1) Every recent agency and private sector breach has had one thing in common: the attacker, once inside the perimeter security, has been able to move freely around the agency’s network. This is a fundamental flaw of network architectures that have proliferated over the past 15 years. The hackers are aware of this flaw and leverage it extensively once inside the network infrastructure.

- 2) Perimeter-centric cyber security policies, mandates, and techniques are critical and necessary, but they are insufficient and ineffective in protecting U.S. Government cyber assets alone.
- 3) These cyber-attacks will continue, but it is possible to significantly and affordably increase our prevention abilities and limit the damage and severity of attacks.

Address the Threat – Immobilize the Attacker

There are many perimeter-centric technologies designed to stop an attacker from getting inside a network, however it is evident that this approach is not sufficient to combat today's cyber-attacks. Perimeter-centric security solutions are analogous to a locked door that can only be accessed with a key. The primary function of the door is to deny initial unauthorized entry by anyone that does not have a key. However, once the door is forced open (hacked or breached), the unauthorized actor is free to move throughout (laterally) unabated.

In another example, imagine a street containing several homes as an analogy for a network containing several servers in a data center. Let's further imagine that there is a corridor that connects every home on the street. If an intruder can manage to break into one home, the intruder now has complete access to all of the other homes on the street even though the doors to the street are locked because there is a trusted passage between them. If the street is long and contains many homes, it has a higher probability that an intruder will be able to access one of those homes and leverage the trusted corridor to access and rob every home on the street, and potentially other streets in the neighborhood. In technology terms, the larger and "flatter" the network, and the more servers on the network, the higher the probability the intruder or hacker will be able to penetrate one server and leverage it to compromise others on that same network. This is what has occurred in most of the private and government cyber attacks in recent months.

In order to effectively prevent an attacker from moving freely around the network, agencies must compartmentalize their networks by creating "Zero Trust" or "micro-segmented" network environments within the data center.

A Zero Trust environment prevents unauthorized "lateral" movement within the data center by establishing automated governance rules that manage the movement of users and data between

business systems and/or applications within the data center network. When a user or system “breaks the rules,” the potential threat incident is compartmentalized and security staff can take any appropriate remediation actions. To build on the analogy above, compartmentalization is equivalent to securing each interior room with locks. Only those with the appropriate keys can move freely within the data center, and the “trusted corridor” is now no longer trusted, and it becomes monitored by automated “guards” who systematically check for and verify correct credentials. Limiting the intruder’s ability to move around freely within the house or through the corridor significantly mitigates the magnitude of a perimeter security breach, or break-in.

While many information technology departments have network segmentation initiatives under way, they are largely insufficient because they use a legacy approach. This legacy approach involves attempting to move perimeter security inside the data center. While these entities tend to achieve some level of segmentation or separation between networks, it is both costly and has limited scalability. In my experience, I find that these organizations discover that this legacy approach does not scale well and becomes overly complex and operationally infeasible. Ironically it leads to reduced security over time. Rather than this legacy approach, a Zero Trust security model should be implemented. This model states that security professionals must eliminate the idea of an internal trusted network and an external untrusted network. In a “zero trust network” all networks are untrusted, meaning there is no “trusted corridor.”

Three concepts underpin “Zero Trust: 1) verify and secure all resources regardless of location, internal or external; 2) limit and strictly enforce access control across all user populations, devices, channels and hosting models; and 3) automatically log and inspect all traffic, both internal and external. This can be automated and performed seamlessly without negatively impacting user response time on the network.

Build the Joint Information Environment (JIE) single security architecture

General Keith Alexander (USA, Ret.), former Director of the National Security Agency and Commander, U.S. Cyber Command, has repeatedly warned of the threats to DoD’s networks: *I look at the DoD Architectures today, and defending them is really hard. We have 15,000 enclaves, each individually managed. The consequence of that is that each one of those is*

*patched and run like a separate fiefdom. The people who are responsible for defending them cannot see down beyond the firewalls. Host-based security systems are helping, but practically speaking, Situational Awareness (SA) is non-existent.*¹

As the Committee is well aware, the Pentagon is building the Joint Information Environment (JIE), a single joint enterprise IT platform that can be leveraged for all DoD missions. It is designed to provide greater standardization and end-to-end visibility with a new single security architecture. We applaud the Department's effort to move to the JIE as it provides a sound framework for enhancing DoD's security posture.

A key recommendation for a successful migration is to leverage the existing cloud based technologies that DoD owns and is in the process of deploying, allowing them to slowly consolidate workloads into the JIE framework. For example, the Air Force is currently leveraging cloud technology to standardize and automate multiple data centers. The Department may want to consider implementing a scorecard to measure and manage the Commands that are making progress to achieve JIE alignment, and leverage their best practices across DoD.

As the Department is implementing its network defense across the enterprise, it should review how it treats unclassified business system networks. Currently these systems, such as email, personnel, and payroll are treated differently than mission critical systems under current DoD practices. As we have seen by recent cyber-attacks on these systems, multiple vulnerabilities on different levels of systems exist today. While many systems may not be deemed mission critical, the impact of a cyber attack on these systems can be just as effective in impairing our ability to defend our nation. Let's assume for a moment that the DoD payroll system was compromised. What would the impacts to troop moral and effectiveness be when their families are not getting their paychecks? These scenarios demonstrate the need for action to ensure all systems are protected. There are proven technologies that can provide the DoD agile tools that can be deployed rapidly in hours or even minutes that can adapt dynamically to the threats. VMware as well as other technology vendors are delivering these technologies to IT companies and the military today.

¹ General Keith Alexander (USA), USCYBERCOM Commander and Director of NSA, "Interview to Federal News Radio," August 24, 2012.

Goal 3: Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence

We recommend two approaches in addressing these initiatives. The first is to automate security features. This will allow the Department to rapidly and dynamically change the countermeasures in place during high threat periods. As stated earlier in my testimony, Zero Trust models are a good example of the security features that can be put into place automatically and used on demand.

The second approach is to use predictive methods to quantify attacks and likely actions based on their early stage. This “cyber kill chain” helps to identify and predict an attacker’s next move. Investing in these capabilities will yield significant benefits by preventing later stage and more serious attacks based on the precursor activities. However, the benefit of these approaches will be reduced if not coupled with on-demand controls and empowerment of our cyber warriors on the front line to use them. This approach can make our cyber defense forces more effective at preventing serious compromises by detecting and stopping these early stage attacks or diverting them to specialists for offensive actions.

Summary

VMware is committed to supporting the U.S. Government’s defense of our national cyber infrastructure. VMware understands the Department’s challenges in addressing the persistent cyber security threat. New cyber security strategies (e.g. Zero Trust or micro-segmentation) that are the current gold standard for commercial industry must become the gold standard for the Department of Defense. To facilitate adoption, government policies should establish ratio metrics for the number of systems/workloads a given system has access to without passing security controls. Today, most government networks have a ratio of 1 to hundreds or 1 to thousands. The target ratio should be 1 to ones or 1 to tens so that if a given network is breached, the damage will be greatly limited. Metrics will enable government policies to better address today’s cyber warfare reality. Additionally, these controls can be adapted dynamically and often automatically to the threat level.

While there is no “silver bullet” to permanently address every cyber security threat, Congress can mandate that agencies adopt policies and security standards that mitigate threats inside the network perimeter.

In summary, the Department of Defense should:

- 1) Establish aggressive automation goals for the management of their IT infrastructure that includes security controls.
- 2) For all existing networks, cut the common thread found in every major breach by implementing a Zero Trust security model and reducing attacker/threat mobility within the network.
- 3) Reward successful organizations when moving to the JIE by sharing best practices within DoD.

VMware sincerely appreciates the opportunity share our thoughts and suggestions on this very important matter. We applaud the leadership and vision of the Chairman and Ranking Member in holding this important hearing. VMware looks forward to continuing to participate in efforts to improve the security of the federal government. Thank you for the opportunity to testify today.

Dominick A. Delfino
Vice President, WW Systems Engineering, Networking & Security Business Unit
VMware

As the Vice President of WW Systems Engineering for the Networking and Security Business Unit, Dominick leads a worldwide team of System Engineers focusing on customer solutions, transformation, and innovation through VMware's strategic technology platforms.

Dominick joined VMware September of 2014 to continue the buildout of the organization and lead the customer facing engineering team chartered with driving Network Virtualization and Security solutions for VMware's customers.

Prior to joining VMware Dominick was a successful fourteen-year veteran of Cisco Systems. Dominick has held a number of positions in the Enterprise, Advanced Technology, and Architecture organizations. Most recently, he was Vice President of Systems Engineering leading the Data Center technology team globally. He was instrumental in pioneering Cisco's data center business, helping to bring to market many of Cisco's most strategic technologies, including MDS, Nexus, and Unified Computing. Dominick's strong leadership helped to drive tremendous growth, leading the technology team in building Cisco's data center business to a \$8B run rate and accelerating Cisco UCS to #2 in x86 blade server market share.

Prior roles included Consulting Systems Engineer in Global Financial Operations, a group that includes some of Cisco's largest enterprise customers, and generates as much as \$500 million in annual revenue for Cisco. While in this position, Dominick consulted with customers on the design and architecture of secure networks, large-scale disaster recovery and business continuity, and metro optical networks. Dominick also successfully architected one of the most mission critical disaster recovery networks on Wall Street for the Depository Trust and Clearing Corporation.

Dominick has presented at industry-wide conferences, providing expertise regarding network security, data center consolidation, and campus network infrastructures. Dominick has also been cited in various technology publications, including Computer Reseller News.

Dominick serves on the board of directors at the Council for Entrepreneurial Development where he advises startup companies.

Dominick studied engineering at the State University of New York, Farmingdale.

**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 114th 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: Dom Delfino

Capacity in which appearing: (check one)

- Individual
- Representative

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

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:

2015

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
Please see attached supplement			

2014

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
Please see attached supplement			

2013

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
Please see attached supplement			

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:

2015

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
Please see attached supplement			

2014

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
Please see attached supplement			

2013

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
Please see attached supplement			

Attachment
 Witness: Don Delfino
 Representing: VMWare, Inc.

Disclosure Form for Witnesses
 Committee on Armed Services
 U.S. House of Representatives

Federal grant/contract	Federal Agency	Subject of contract or grant	Dollar Value
2015			
DJF153100P00100174	FEDERAL BUREAU OF INVESTIGATION	ADP SOFTWARE	\$0.00
DJF153100P00100174	FEDERAL BUREAU OF INVESTIGATION	ADP SOFTWARE	\$3,811.04
HHSP23300100186P	PROGRAM SUPPORT CENTER	OFFICE INFORMATION SYSTEM EQUIPMENT	(\$5,881.00)
DJF141100P0010702	FEDERAL BUREAU OF INVESTIGATION	ADP CENTRAL PROCESSING UNIT (CPU, COMPUTER), DIGITAL	(\$40,760)
TFSAJCFP150040	BUREAU OF THE FISCAL SERVICE	EDUCATION/TRAINING- TUITION/REGISTRATION/MEMBERSHIP FEES	\$5,085.00
HHSP23300100123A	PROGRAM SUPPORT CENTER	ADP SOFTWARE	(\$6,812.00)
ADZ7801400940	AGENCY FOR INTERNATIONAL DEVELOPMENT	IT AND TELECOM-ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS	\$0.00
ING15P000091	GEOLOGICAL SURVEY	IT AND TELECOM-ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS	\$12,761.01
HHSD2470150024A	INDIAN HEALTH SERVICE	ADP SOFTWARE	\$13,884.80
2014			
	Federal Agency	Subject of contract or grant	Dollar Value
DJF142200P003360	FEDERAL BUREAU OF INVESTIGATION	ADP SOFTWARE	(\$299.95)
ADZ7801400940	AGENCY FOR INTERNATIONAL DEVELOPMENT	IT AND TELECOM-ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS	\$5,101.16
INR14P000886	BUREAU OF RECLAMATION	IT AND TELECOM-ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS	\$0.00
HHSD247201400106A	INDIAN HEALTH SERVICE	ADP SOFTWARE	\$12,858.71
INR14P000886	BUREAU OF RECLAMATION	IT AND TELECOM-ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS	\$24,501.60
N668044493373	DEPT OF THE NAVY	EDUCATION/TRAINING- TUITION/REGISTRATION/MEMBERSHIP FEES	\$1,995.00
CNSIG14P0001	CORPORATION FOR NATIONAL AND COMMUNITY SERVICE	IT AND TELECOM- IT STRATEGY AND ARCHITECTURE	\$21,312.06
DJF141100P0010702	FEDERAL BUREAU OF INVESTIGATION	ADP CENTRAL PROCESSING UNIT (CPU, COMPUTER), DIGITAL	\$166.60
SE105A13P0049	DEFENSE CONTRACT MANAGEMENT AGENCY (DCMA)	ADP SOFTWARE	\$409,366.90
STH20014M1835	STATE, DEPARTMENT OF	ADP SOFTWARE	\$5,241.00
DOLE49435567	OFFICE OF THE ASSISTANT SECRETARY FOR ADMIN AND MANAGEMENT	ADP SOFTWARE	\$9,945.90
DJF142200P003369	FEDERAL BUREAU OF INVESTIGATION	ADP SOFTWARE	\$299.95
EP145000021	ENVIRONMENTAL PROTECTION AGENCY	IT AND TELECOM- DATA CENTERS AND STORAGE	\$15,984.00
2013			
	Federal Agency	Subject of contract or grant	Dollar Value
ND13P00004	OFFICE OF POLICY, MANAGEMENT, AND BUDGET	IT AND TELECOM-ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS	\$3,819,905.60
W97505C4762	DEPT OF THE NAVY	IT AND TELECOM- OTHER IT AND TELECOMMUNICATIONS	\$0.00
ADG00170056	DEPT OF THE NAVY	IT AND TELECOM- OTHER IT AND TELECOMMUNICATIONS	\$97,665.00
SE105A13P0049	DEFENSE CONTRACT MANAGEMENT AGENCY (DCMA)	ADP SOFTWARE	\$409,366.00
CNSIG13P21228	CORPORATION FOR NATIONAL AND COMMUNITY SERVICE	IT AND TELECOM- IT STRATEGY AND ARCHITECTURE	\$0.00
N0017313P21462	DEPT OF THE NAVY	MAINT/REPAIR/REBUILD OF EQUIPMENT-ADP EQUIPMENT/SOFTWARE/SUPPLIES/SUPPORT EQUIPMENT	\$3,295.00
AG3444P130444	USDA, OFFICE OF THE CHIEF FINANCIAL OFFICER	EDUCATION/TRAINING- OTHER	\$6,152.00
FTCL13M3117	FEDERAL TRADE COMMISSION	ADP SOFTWARE	\$4,800.00
N0016813P3705	DEPT OF THE NAVY	MEDICAL AND SURGICAL INSTRUMENTS, EQUIPMENT, AND SUPPLIES	(\$1,875.30)
HHSD26301300428P	NATIONAL INSTITUTES OF HEALTH	IT AND TELECOM-ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS	\$4,965.28
DOL8139A34461	OFFICE OF THE ASSISTANT SECRETARY FOR ADMIN AND MANAGEMENT	ADP SOFTWARE	\$24,307.30
HHSD202010M37509P	CENTERS FOR DISEASE CONTROL AND PREVENTION	ADP COMPONENTS	\$0.00
N0016813P3705	DEPT OF THE NAVY	MEDICAL AND SURGICAL INSTRUMENTS, EQUIPMENT, AND SUPPLIES	\$0.00
N0017313P0523	DEPT OF THE NAVY	MEDICAL AND SURGICAL INSTRUMENTS, EQUIPMENT, AND SUPPLIES	\$3,790.00
DOCDC1360105U1761	NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION	MAINT/REPAIR/REBUILD OF EQUIPMENT- ADP EQUIPMENT/SOFTWARE/SUPPLIES/SUPPORT EQUIPMENT	\$0.00
N0017313P0523	DEPT OF THE NAVY	IT AND TELECOM- SYSTEMS DEVELOPMENT	\$4,000.00
N0016813P0664	DEPT OF THE NAVY	MAINT/REPAIR/REBUILD OF EQUIPMENT- ADP EQUIPMENT/SOFTWARE/SUPPLIES/SUPPORT EQUIPMENT	\$16,754.00
W91QZJ2P0064	DEPT OF THE ARMY	IT AND TELECOM-ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS	\$0.00

Perspective on 2015 DoD Cyber Strategy

Lara Schmidt

RAND Office of External Affairs

CT-439

September 2015

Testimony presented before the House Armed Services Committee on September 29, 2015

This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. RAND® is a registered trademark.



Published 2015 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: <http://www.rand.org/>
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Email: order@rand.org

Lara Schmidt¹
The RAND Corporation

*Perspective on 2015 DoD Cyber Strategy*²

Before the Committee on Armed Services
United States House of Representatives

September 29, 2015

Chairman Thornberry, Ranking Member Smith, and distinguished members of the House Armed Services Committee, thank you for inviting me here today to testify at this important hearing, "Outside Perspectives on the Department of Defense Cyber Strategy."

In April 2015, the DoD released a new cyber strategy in order to "guide the development of DoD's cyber forces and strengthen [its] cyber defense and cyber deterrence posture."⁴ The Strategy identifies three cyber missions for DoD: (1) defending its own networks, systems, and data; (2) defending U.S. national interests against cyberattacks of "significant consequence," including loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, and serious economic impact; and (3) when directed by the President or Secretary of Defense, supporting military operations and contingency plans with cyber operations, including by disrupting an adversary's military-related networks.

DoD further laid out strategic goals aimed at ensuring its ability to accomplish these cyber missions, including goals to:⁵

- Build and maintain ready forces and capabilities to conduct cyber operations;
- Defend DoD networks, secure DoD data, and mitigate risks to DoD missions;
- Build and maintain viable cyber options, and plan to use them to control conflict escalation and shape the conflict environment at all stages.

¹ The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

² This testimony is available for free download at <http://www.rand.org/pubs/testimonies/CT439/>.

⁴ Department of Defense, *The DoD Cyber Strategy*, April 2015.

⁵ Two additional goals of the DoD Cyber Strategy not discussed in this Testimony are: (a) Be prepared to defend the U.S. homeland and U.S. vital interests from cyberattacks of significant consequence; and (b) Build and maintain international alliances and partnerships to deter shared threats and increase international security and stability.

Implementation initiatives – and the attendant resources – to achieve these goals are needed in order to meet challenges associated with the rapid rate of change in technology, the growing cyber threat, and the need to integrate cyber operations with operations in other warfighting domains.

Cyber Workforce

Building and maintaining a qualified workforce underlies all of the goals of the *Strategy*. However, U.S. Cyber Command reports that it is “hard pressed” to identify, train, and retain qualified personnel.⁶ How can DoD ensure a ready-workforce of military, civilian, and contractor personnel, capable of meeting the demands of the nation? Like the commercial sector, DoD requires staff to perform IT functions (e.g., configure databases, install and manage applications, provide customer support, securely configure networks, test new designs, develop system architectures), and cybersecurity functions (e.g., identify and analyze network intrusions or other threats, develop security tools, respond to security emergencies, assess threats and vulnerabilities and remediate risk).⁷ Furthermore, DoD requires specialized workforces associated with military cyber operations that are not commonly found in the commercial sector, though applicable skillsets overlap to some extent with elite commercial cybersecurity personnel. How can DoD compete with the rest of the technology sector – e.g., cybersecurity companies, software and hardware developers, the defense industrial base, not to mention IT departments in companies across the country – also seeking to identify an educated and capable workforce? It is helpful to understand how the commercial sector identifies staff.

Commercial practice is to hire cyber staff with a bachelor’s degree, which provides a strong foundation of relevant knowledge, and demonstrates an ability to succeed in a professional setting. Companies usually recruit graduates of reputable colleges with STEM degrees – science, technology, engineering, and mathematics – especially computer science, information security, information technology, computer engineering, and electrical engineering.⁸ However, unlike the commercial sector, the majority of DoD’s military cyber workforce is enlisted and, therefore, not typically required to have college degrees. Therefore, DoD will need to implement substantially more-rigorous selection criteria in order to vet non-degreed candidates to ensure enlisted accessions and new civilian hires are likely to succeed in the cyber workforce. For example,

⁶ Admiral Michael Rogers, Statement before the House Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, 4 March 2015.

⁷ National Initiative for Cybersecurity Careers and Studies, *Interactive national Cybersecurity Workforce Framework*, Washington, D.C.: Department of Homeland Security, undated.

⁸ Schmidt, Lara and Caoliann O’Connell et al, *Cyber Practices: What Can the U.S. Air Force Learn from the Commercial Sector?*, Santa Monica, Calif.: RAND Corporation, RR-847-AF, 2015.

cyber aptitude- or skills-testing or possession of professional certificates⁹ can evaluate a candidate's expertise or mind-set for a particular discipline. Participation in activities such as, cyber competitions, open-source or ethical-hacker forums, or bug bounty programs can indicate a personal interest in and affinity for cyber. In fact, commercial practice for elite, highly paid cybersecurity jobs is to screen for such indications of aptitude and affinity *in addition to* formal educational requirements. These practices merit evaluation for implementation in DoD to ensure military and civilian staff are qualified to meet the challenges the Department faces.

Furthermore, the commercial sector reports that their ability to *retain* skilled personnel is closely linked to job satisfaction gained through good working environments, belief in the mission, opportunities for training and professional development, and access to interesting assignments. Research indicates that corporate retention programs also seek to provide satisfying career paths for their cyber workforces, including not only a track to promotion through management but also a technical track. They also provide high performers opportunities to rotate among units to learn the business, and exposure to professional interaction outside the company.¹⁰

Though some worry that DoD hiring and retention suffers because it cannot keep pace with commercial pay, median salaries for corporate IT and cybersecurity professionals are similar to the pay and benefits for military personnel, when accounting for additional allowances and tax advantages.¹¹ One exception relates to the most elite cybersecurity professionals, those with unique skills that few possess (e.g., software reverse engineering, advanced malware analysis, identifying advanced stealthy attacks). These cyber "ninjas" are the competitive advantage for cutting-edge cybersecurity firms and are increasingly in demand in other corporate settings. The relative scarcity of these skill sets allows qualified individuals to command high salaries.¹² Therefore, DoD might similarly find personnel with these unique skills to be worthy of retention programs not offered to the majority of the cyber workforce.¹³

⁹ To name just a few: Microsoft Certified Solutions Expert (MSCE), Certified Information Systems Security Professional (CISSP), or Certified Ethical Hacker (CEH).

¹⁰ Schmidt, 2015; James Kaplan, Naufal Khan, and Roger Roberts, "Winning the Battle for Technology Talent," McKinsey & Company, May 2012.

¹¹ Based on assessment of: Office of the Under Secretary of Defense for Personnel and Readiness, "Regular Military Compensation Calculator," undated; and Bureau of Labor Statistics, *Occupational Outlook Handbook*, Washington, D.C., January 8, 2014.

¹² There is a "rising difficulty of finding and retaining qualified individuals at what are considered reasonable wages ... at the high end of the capability scale: roughly the top 1–5 percent of the overall workforce. These are the people capable of detecting the presence of advanced persistent threats, or, conversely, finding the hidden vulnerabilities in software and systems that allow advanced persistent threats to take hold of targeted systems." Martin C. Libicki, Dave Senty, and Julia Pollak, *Hackers Wanted: An Examination of the Cybersecurity Labor Market*, Santa Monica, Calif.: RAND Corporation, RR-430, 2014.

¹³ Other specialties such as pilots already receive retention incentives to compete with strong competition in the commercial sector.

To build and maintain a *ready-workforce*, personnel will need to be able to keep up with the pace of technological change. Technology skills – such as programming and knowledge of hardware and software – are perishable.¹⁴ Once such skills have been developed through training, career progression must foster the retention of technical depth. Both *specialization* and *recurring training* merit attention as approaches to ensure the readiness of cyber forces. Specialization reduces the universe of possible technology trends with which personnel must keep pace. By managing staff to maintain specializations in either DoD Information Network (DoDIN) operations, or cyber operations (defensive, offensive)),¹⁵ the DoD may reap effectiveness and efficiency gains. Particularly for military personnel with frequent changes in assignments, maintaining depth and currency will depend upon the similarity of the skillsets required from one position to the next. Furthermore, aligning military specialty codes and civilian occupation codes with duties requiring like-skillsets (e.g., as described in the National Initiative for Cyberspace Education's (NICE) Cybersecurity Workforce Framework¹⁶) enables an approach to personnel management consistent with fostering technical depth. Jobs that require the greatest technical depth and longevity may merit assignment of civilians, guard, and reserve personnel. Guard and reserve personnel may be particularly effective if they are also able to keep their technical skills sharp by working in a cyber-relevant civilian profession while not activated.

Finally, it is important to remember that despite DoD's growing emphasis on offensive and defensive cyber operations, the bulk of the DoD workforce is involved in the day-to-day job of securely configuring, monitoring, and maintaining DoD software applications and computer software and networks. Ensuring the availability of these networks and systems is vital to DoD. In addition, the duties, operational conditions, skillsets needed (and thus, training required) for this DoDIN workforce differ from those conducting offensive and defensive cyber operations. Therefore, maintaining a ready-workforce also requires investment to ensure the currency and capacity of those assigned to the DoDIN mission area.

¹⁴ National Research Council, *Building a Workforce for the Information Economy*, Washington, D.C.: The National Academies Press, 2001; Timothy R. Homan and Zachary Tracer, "ADP Estimates Companies in U.S. Added 42,000 Jobs," *Bloomberg*, August 4, 2010. Martin C. Libicki, Lillian Ablon and Tim Webb, *The Defender's Dilemma: Charting a Course Toward Cybersecurity*. Santa Monica, CA: RAND Corporation, 2015.

¹⁵ Joint Staff, *Cyberspace Operations*, JP 3-12(R), 5 February 2013.

¹⁶ National Initiative for Cybersecurity Education, *National Cybersecurity Workforce Framework*, Washington, D.C.: Department of Commerce, 2013. Note that the *Strategy* specifically calls out a goal to support the NICE initiative.

Cyber Risk Management

DoD has mandated a risk management approach to secure its systems across their lifecycle,¹⁷ based on the NIST Risk Management Framework.¹⁸ Adopting this risk management approach requires an evaluation of the ability of adversaries to attack DoD systems and, more importantly, an assessment of whether such attacks are likely to succeed (e.g., due to the presence of vulnerabilities in DoD systems, or weaknesses in DoD security processes, architecture designs, or supply chains), and the impact a successful attack would have on DoD missions. In particular, such efforts must trace mission activities to the cyber systems they rely on, and identify any vulnerabilities or weaknesses that could be successfully exploited. Therefore, managing risk holistically across the Department promises to be challenging to implement for several reasons.

First, assessing vulnerabilities and weaknesses associated with all DoD systems – to include IT and business systems, and the computer components of DoD weapon systems – is no small feat due to the number of such systems in existence. Furthermore, even given assessed levels of risk for all DoD systems, decision-makers may find it challenging to prioritize risk mitigation efforts due to *uncertainties* about whether high risk systems will be attacked and how the functionality of such systems weighs on the ability to conduct missions in the range of conditions the military could potentially experience (from peacetime to war). Finally, cyber risk changes over time as systems are upgraded or new attacks are enabled by newly discovered vulnerabilities; therefore risk assessments need to be conducted with sufficient regularity to keep up with the pace of change.

Given these challenges, a *practical* risk management implementation plan is necessary. The *Strategy's* objective to “mitigate all known vulnerabilities that present a high risk to DoD networks and data” is a laudable goal, however further work is likely to be required to define specifically how high-risk vulnerabilities will be identified and how risk mitigation efforts can be prioritized and facilitated. DoD acknowledges that it cannot mitigate *every* risk, thus there are likely to be some successful attacks. Contingency plans and resilience strategies to maintain critical missions in the wake of such attacks, and consequence management initiatives to quickly eject attackers from critical networks are key implementation objectives of the *Strategy*.

¹⁷ Department of Defense, “Risk Management Framework (RMF) for DoD Information Technology (IT),” DoDI 8510.01, 12 March 2014.

¹⁸ National Institute of Standards and Technology, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,” NIST SP-800-37 Revision 1, February 2010.

Academic cybersecurity researchers have rightly noted that knowing of the existence of vulnerabilities or even the severity¹⁹ of these vulnerabilities is not enough to know what systems will be successfully attacked.²⁰ Instead, they recommend augmenting vulnerability and severity information with actual “field data” from systems and big-data analytic techniques to understand attack trends on both known and previously unrecognized vulnerabilities. DoD is in an ideal position to collect data on its fielded systems; however, such data would need to be analyzed and linked to mitigation options as risks are discovered. Doing so merits consideration as part of a practical risk management implementation plan for DoD.

Deliberate Planning for Cyber Operations

Historically, to achieve warfighting objectives, the conventional targeting process was designed to select and prioritize targets and match the appropriate conventional weapon based on operational requirements and available capabilities.²¹ Part of doing so is estimating the likelihood that weapons will perform as intended and result in the desired effects (and avoid undesired effects such as collateral damage). Decades of research and development has resulted in a robust capability to make such estimates for conventional weapons, grounded by physics models and extensive testing data. This targeting process and its ability to estimate weapon effects have greatly facilitated construction of military operational plans.

Now, the *DoD Cyber Strategy* is calling for increased integration of cyber operations into such plans to help meet desired strategic end-states.²² Integrating cyber with conventional operations, therefore, requires measures of the likelihood that cyber operations will succeed against their intended targets.²³ While the physics-based models so prevalent in conventional targeting are not applicable to cyber, the *scientific approach* used to develop a rigorous process for estimating weapon effects can and should be replicated for cyber operations. That is, large-scale analytic efforts to understand the performance of cyber operations in a variety of operational conditions

¹⁹ For example, lists of known vulnerabilities and the commercial software/hardware systems that are affected are available, e.g., the NIST National Vulnerability Database, which also includes an indication of the severity of the vulnerability as assessed by the Common Vulnerability Scoring System.

²⁰ Tudor Dumitras, “Understanding the Vulnerability Lifecycle for Risk Assessment and Defense Against Sophisticated Cyber Attacks,” Chapter 13 in *Cyber Warfare: Building the Scientific Foundation*, Edited by Sushil Jajodia, Paulo Shakarian, V.S. Subrahmanian, Vipin Swarup, and Cliff Wang, New York: Springer, 2015.

²¹ Joint Staff, “Joint Operations,” JP 3-0, 11 August 2011.

²² The Strategy highlights the need to “define specific cyberspace effects against targets,” for example to “disrupt an adversary’s military-related networks and infrastructure.”

²³ Mark Gallagher and Michael Horta, “Cyber Joint Munitions Effectiveness Manual (JMEM),” *M&S Journal*, Summer 2013, pp. 5-13.

are needed to enable informed decision-making about the potential for cyber operations to contribute to warfighting objectives and avoid undesired effects. This includes significant testing, data collection, and analysis efforts.

Furthermore, any scientific approach must be tailored to the complexities and uncertainties associated with cyber operations. For example, details about the path between attacker and target, the configuration of the target computer, its defenses, and the behaviors of adversary network defense personnel all affect whether an attack will succeed or fail. Expanding target descriptions to include such aspects relevant to cyber targeting must do so in a way that is tractable given the shorter time periods over which cyber configurations may remain stable on any given target.²⁴ Nonetheless, successfully integrating cyber operations into DoD deliberate planning activities will require a well-resourced, rigorous approach to estimating the effectiveness of potential future cyber operations.

Conclusion

In conclusion, it is my opinion that the *DoD Cyber Strategy* lays out an ambitious set of goals that are well aligned with operationalizing cyber. However, implementing the initiatives needed to achieve these goals will be challenging due to the difficulties in quickly building and maintaining a capable workforce, assessing risk across the large number of DoD networks and systems, and planning for operations in this highly dynamic environment.

I appreciate the opportunity to discuss this important topic and I look forward to your questions.

²⁴ *ibid*

Lara Schmidt
Associate Director, RAND Project AIR FORCE; Senior Statistician
Santa Monica Office

Education

Ph.D. in statistics, American University; M.S. in mathematics, West Virginia University; B.S. in mathematics, Shepherd College

Lara Schmidt is a senior statistician at the RAND Corporation. She serves as the associate director of RAND Project AIR FORCE, the Air Force's federally funded research and development center (FFRDC) for studies and analysis. She manages the FFRDC's quality assurance efforts and leads studies as a senior member of the research staff. Her work focuses on national security space and cyber systems, threats to these systems, and the associated risk to the warfighter. Her recent work includes assessments of the cyber risk to command and control, Air Force special operations and irregular warfare, integrating cyber operations into the Joint targeting cycle, and Air Force weapons mix planning. Schmidt serves as a referee for several technical journals and has held leadership positions with the American Statistical Association, including serving as the Chair of the ASA Section on Statistics in Defense and National Security. Prior to joining RAND, she spent eight years as a government civilian working in GPS and atomic timekeeping. Schmidt holds B.S. and M.S. degrees in mathematics and a Ph.D. in mathematical statistics from American 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 114th 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: Lara Schmidt

Capacity in which appearing: (check one)

Individual

Representative

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

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:

2015

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
Contract	U.S. Air Force	\$39,025,435	PROJECT AIR FORCE
Contract	DoD	\$48,882,351	NDRI

2014

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
Contract	U.S. Air Force	\$46,055,801	PROJECT AIR FORCE
Contract	DoD	\$63,759,733	NDRI

2013

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
Contract	U.S. Air Force	\$34,399,281	PROJECT AIR FORCE
Contract	DoD	\$63,539,233	NDRI

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:

2015

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
Please see attached supplement			

2014

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
Please see attached supplement			

2013

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract or payment
Please see attached supplement			

Federal Contract or Grant Information

The RAND Corporation is an independent, non-profit organization that performs research and analysis. During the time period in question (FY2013 through fiscal year 2015), RAND has had contracts and grants with various agencies of the federal government to perform research and analysis. Research has been performed for the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Justice, Treasury, Veterans Affairs, the Administrative Office of the United States Courts, the Centers for Disease Control and Prevention, the National Institutes of Health, the Environmental Protection Agency, the Federal Communications Commission, the Federal Reserve Banks of Boston and New York, the Intelligence Community, the Medicare Payment Advisory Commission, the National Aeronautics and Space Administration, the National Science Foundation, the Social Security Administration, and the U.S.-China Economic and Security Review Commission. RAND has contracts with the Department of Defense to operate three federally funded research and development centers (FFRDC): PROJECT AIR FORCE for the U.S. Air Force; Arroyo Center for the U.S. Army; and National Defense Research Institute for the Department of Defense.

Foreign Government Contract or Payment Information**FY15**

Foreign Contract/Payment	Foreign Government	Dollar Value	Subject of contract or payment
Contract	Commonwealth of Australia	\$6,512,435	Research
Contract	Canada	\$21,883	Research
Contract	Japan	\$25,000	Research
Contract	Korea	\$100,000	Research

FY14

Foreign Contract/Payment	Foreign Government	Dollar Value	Subject of contract or payment
Contract	Commonwealth of Australia	\$3,923,158	Research
Contract	Japan	\$190,000	Research
Contract	Instituto De Nutricion De Centro America y Panama	\$16,300	Research
Contract	Israel	\$59,175	Research

Contract	Kurdistan Regional Government	\$3,040,001	Research
Contract	Mongolia	\$750,000	Research

FY13

Foreign Contract/Payment	Foreign Government	Dollar Value	Subject of contract or payment
Contract	Arab Administrative Development Organization	\$575,000	Research
Contract	Commonwealth of Australia	\$3,000	Research
Contract	Instituto De Nutricion De Centro America y Panama	\$10,000	Research
Contract	Israel	\$64,000	Research
Contract	Kurdistan Regional Government	\$2,995,219	Research
Contract	Republic of Korea	\$104,015	Research
Contract	Republic of Singapore	\$444,500	Research
Contract	Mexico	\$22,845	Research
Contract	Department of House and Urban Development Guangdong Province - Peoples Republic of China	\$800,000	Research
Contract	Switzerland	\$10,000	Research
Contract	Thailand	\$20,900	Research
Contract	Qatar	\$296,127	Research

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

SEPTEMBER 29, 2015

QUESTIONS SUBMITTED BY MR. SHUSTER

Mr. SHUSTER. In your testimony, you said you do not support giving private sector, non-government parties the authority to conduct offensive operations. At what point do you think it becomes appropriate for the U.S. Government to investigate, prosecute, or defend private sector entities?

Mr. BEJTICH. Private sector entities must comply with local, state, and federal laws governing breach disclosure, particularly with regard to loss of personally identifiable information. Beyond cases that involve mandatory disclosure, private sector entities make decisions by weighing the costs and benefits of engaging law enforcement. I personally encourage private sector entities to contact law enforcement because such engagement helps law enforcement build cases against perpetrators, ultimately contributing to their arrest and prosecution. Law enforcement should investigate and prosecute whenever they learn of an incident and can make a case.

Mr. SHUSTER. You mentioned that VMware serves all sectors of the U.S. Government to include DOD, civilian agencies and the Intelligence Community. I recognize that each entity must develop a comprehensive cyber strategy yet I worry that differing strategies among our government entities could create challenges for companies like VMware that works across agencies. What issue areas are best legislated by Congress for the whole of government and what areas would you defer to DOD and/or other executive agencies to develop?

Mr. DELFINO. Congress can assist the efforts of developing a comprehensive cyber strategy by providing adequate funding for training of cyber employees to defend our nation. Experienced talent in cybersecurity is a specialized skill and Congress can encourage the use of special hiring authorities to pay experienced personnel competitive private sector rates. Congress can also assist agencies and the private sector in being better informed about cyber threats by passing laws that enhance government and private sector information sharing. Since technology is changing so rapidly, Congress should not legislate technology mandates but rather encourage the use of best practices that the private sector is adopting. In order to ensure the government has a comprehensive strategy, the Office of Management and Budget and the National Security Council should work across the civilian and defense agencies to set procedures, best practices, and metrics that the agencies can follow. Congress can assist these efforts by providing oversight and highlight the Executive Branch's progress or challenges.

Mr. SHUSTER. In your written testimony, you addressed DOD shortfalls in both recruiting and retention of the cyber workforce. Often times, financial incentives are cited as the potential solution to these shortcomings. I agree with your statement that retention is closely linked to job satisfaction so my question is whether DOD's human capital management system is effective in placing the cyber workforce into positions that provide sufficient skill utilization and job satisfaction?

Dr. SCHMIDT. I have not conducted a formal analysis of the extent to which the Department of Defense's (DOD's) approach to cyber workforce management succeeds in placing civilians and service members into jobs for which they are qualified. Furthermore, I am unaware of any such assessment for workforce management approaches following the new initiatives DOD unveiled in 2015.¹ However, the work undertaken as part of the National Initiative for Cyberspace Education (NICE) Cyberspace Workforce Framework,² which identifies the required skills for many cyberspace jobs, is a necessary first step toward performing any "job analysis" to evaluate the extent to which personnel matched to jobs possess the required skills to work effectively. Both receiving the right training (initial and continuing) and progressing through different jobs that draw on similar skill sets are important to ensuring personnel are well matched to job requirements.

I am also unaware of any formal analyses of job satisfaction among DOD's civilian and military cyberspace cadres. Conventional wisdom asserts that DOD offers its

¹Department of Defense, Cyberspace Workforce Management, Directive 8140.01, August 11, 2015.

²NICE, National Cybersecurity Workforce Framework, Washington, D.C.: Department of Commerce, 2013. The services have adopted this framework to varying extents.

personnel unique opportunities to serve the nation and conduct high-stakes, highly dynamic operations they would find no place else; as a result, conventional wisdom asserts that job satisfaction is high. While this assertion rings true for some DOD cyberspace jobs (e.g., military personnel conducting offensive and defensive operations), I question the wisdom of applying such logic to DOD cyberspace jobs that both (a) require staff to manage a high operational tempo and other stressors on family and personal time (e.g., frequent changes of duty location and/or organizations) and (b) are similar to jobs conducted in the private sector (i.e., lack the “only in DOD” allure). Therefore, an assessment of job satisfaction in the “IT-like” DOD Information Network Operations (DODIN Ops) job categories may be illuminating, as it may not adhere to conventional wisdom. Commercial-sector IT job satisfaction has been linked to the existence of defined career paths that allow growth and progression not only through advancement into the management ranks, but also through technical tracks that allow personnel to continue to learn, engage with professional peer groups, and innovate to keep pace with rapidly changing technology.

QUESTIONS SUBMITTED BY MR. WALZ

Mr. WALZ. There are several ongoing cyber initiatives between the National Guard and private sector. Are any of you familiar with any of these initiatives? If so, could you comment on the opportunity the Federal Government and DOD has to benefit from the lessons learned by these initiatives?

Mr. BEJTICH. I am not deeply familiar with specific initiatives. However, I have observed National Guard cyber exercises involving teams from across the country. Although I saw a wide variety in the capabilities of the teams, some operated at very high levels. All were motivated to improve their skills. I believe that National Guard and Reserve components are part of the answer to better defense at a national level. However, I also believe the government should support research projects to evaluate the costs and benefits of an independent military Cyber Force.

Mr. WALZ. There are several ongoing cyber initiatives between the National Guard and private sector. Are any of you familiar with any of these initiatives? If so, could you comment on the opportunity the Federal Government and DOD has to benefit from the lessons learned by these initiatives?

Mr. WALLACE. [No answer was available at the time of printing.]

Mr. WALZ. There are several ongoing cyber initiatives between the National Guard and private sector. Are any of you familiar with any of these initiatives? If so, could you comment on the opportunity the Federal Government and DOD has to benefit from the lessons learned by these initiatives?

Mr. DELFINO. Yes, VMware is working with the National Guard Bureau at the Professional Education Center in Little Rock, Arkansas. We are helping the National Guard Bureau architect a cyber “Classroom as a Service” experience that allows cyber warrior training to be stood up in minutes and allows for realistic threat scenarios. This is based on the model VMware implemented at US Army Cyber Center of Excellence in Fort Gordon, Georgia.

Mr. WALZ. Do you believe DOD has a complete and comprehensive strategy for cyber policy? If not, what level of vulnerability risk would you estimate the DOD and Federal Government networks to be at, high, medium, or low?

Dr. SCHMIDT. [No answer was available at the time of printing.]

Mr. WALZ. There are several ongoing cyber initiatives between the National Guard and private sector. Are any of you familiar with any of these initiatives? If so, could you comment on the opportunity the Federal Government and DOD has to benefit from the lessons learned by these initiatives?

Dr. SCHMIDT. [No answer was available at the time of printing.]

Mr. WALZ. Including the data breach at OPM and the Joint Chiefs of Staff server, there have been several high profile government cyber breaches in the last year. Are these network compromises a result of lack of technical capability in the cyber workforce, or a lack of cyber policy that prioritizes protections? In your opinion, what actions would you recommend are the most important to take in reducing the likelihood of future data breaches and protect our cyber networks?

Dr. SCHMIDT. [No answer was available at the time of printing.]