SEPTEMBER 29, 2015

OUTSIDE PERSPECTIVES ON THE DEPARTMENT OF DEFENSE CYBER STRATEGY

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON ARMED SERVICES, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

ONE HUNDRED FOURTEENTH CONGRESS, FIRST SESSION

HEARING CONTENTS:

MEMBER STATEMENTS:

WITNESSES:

AVAILABLE WEBCAST(S):

Full Hearing: *https://youtu.be/q99nzK6lxeU?t=109*

COMPILED FROM:

http://armedservices.house.gov/index.cfm/hearings-display?ContentRecord_id=687057FD-ACCC-4119-87A9-DEE9DBA130B8&ContentType_id=14F995B9-DFA5-407A-9D35-56CC7152A7ED&Group_id=64562e79-731a-4ac6-aab0-7bd8d1b7e890

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

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.

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.

Testimony

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

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 Schmidt[1]
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 Caolionn 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 certificates[9] 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 Framework[16]) 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 severity[19] 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

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 Strategy[4], 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.