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