Communications of the IIMA

Volume 16 | Issue 2 Article 2

2018

Cyber Capability Planning and the Need for an Expanded Cybersecurity Workforce

Tony Coulson
California State University - San Bernardino, tcoulson@csusb.edu

Megan Mason
California State University - San Bernardino

Vincent Nestler
California State University - San Bernardino, vnestler@csusb.edu

INTRODUCTION

Cybersecurity is a rapidly developing field designed to protect information systems from continual risk. Cybersecurity has been at the forefront of conflicts, politics, and both enterprise and military attacks. Cyber threats present unique concerns for all governments, including challenges to their ability to operate and defend critical systems. This paper provides an overview of the important role that cybersecurity has in the United States, framed by military capability planning, and explains how mass workforce development models, such as the National Initiative for Cybersecurity Education (NICE) Capability Maturity Model and NICE Framework, provide a methodology to enhance human resource capabilities. Furthermore, this work examines several initiatives designed to provide for national cybersecurity needs and suggests how a well-equipped cybersecurity workforce can be enhanced by using strategic recruitment and building a talent pipeline.

Important Cyber Challenges

In February 2017, the Department of Defense Science Board (DSB) released a report titled *Task Force on Cyber Deterrence* that raised several concerns. First, the agency recognized that the U.S. military has an extensive dependence on information technology, which creates a massive attack surface. Second, the report noted that major powers such as Russia and China have an increasing capacity to hold U.S. critical infrastructure at risk or to use information they gather to damage vital U.S. interests. Though currently limited, foes' ability to obstruct United States' military responses through cyberattacks continues to develop (Department of Defense Science Board [DSB], 2017).

The DSB concluded that the offensive cyber capabilities of the United States' adversaries are likely to "far exceed the United States' ability to defend and adequately strengthen the resilience of its critical infrastructures" in the coming five to ten years (DSB, 2017). Therefore, it is necessary for the United States to improve its cyber posture to mitigate the extensive vulnerabilities to nations such as Russia, China, North Korea, and others. Although the results of the DSB report focus on the United States, it is critical for U.S. allies to strengthen their cyber capabilities as well. The majority of serious militaries around the world either have cyber capabilities or they desire to develop such abilities (Wallace, 2013). As a result, having a framework to help military cyber capability planning is an area in which a more refined system is necessary.

Military Cybersecurity Capabilities: "Leverage the Nation's Ingenuity Through an Exceptional Cyber Workforce"

Militaries play an important role in national cybersecurity governance. In 2011, the United States Department of Defense (DoD) released a document defining its strategy for operating in cyberspace. The plan consists of five strategic initiatives. The first is to treat cyberspace as an operational domain that should be organized, educated, and prepared to ensure DoD's capability to take advantage of cyberspace's potential. The second step is to "employ new defense operating concepts to protect Department of Defense networks and systems." The third strategic initiative is for the DoD to partner with other U.S. government departments and agencies, as well as the private sector, to enable a "whole-of-government cybersecurity strategy." This would include developing new capabilities and supporting collective efforts among government agencies, Internet Service Providers, and global supply chains. The fourth strategic initiative is to build a robust relationship with U.S. allies and international partners to increase collective cybersecurity. The final initiative is to "leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation" (DoD, 2011). These strategies are important to national security, which is being redefined by cyberspace, in the United States and other countries. Although cyberspace provides opportunities to militaries, it also presents significant challenges. As a result, the recommended strategic initiatives would allow the DoD to capitalize on the opportunities within cyberspace, focus on protecting networks and systems from intrusions, and build strong cyberspace capabilities

Capability-Based Planning. There are several definitions of capability-based planning (CBP). CBP can be defined as a systematic technique applied to "functional analysis of operational requirements" in which capabilities are identified based on a set of requirements and then satisfied using the most cost-effective options available (The Technical Cooperation Program Joint Systems and Analysis Group [TCPJSAG], n.d.). CBP has also been referred to as the "planning, under uncertainty, to provide capabilities suitable for a wide range of modern-day challenges and circumstances while working within an economic framework that necessitates choice" (TCPJSAG, n.d.). CBP was "developed as an alternative to threat-based planning" (TCPJSAG, n.d.). Threat-based planning is developing plans with "clear and identifiable benchmarks" (Balasevicius, 2016) based on an identifiable enemy enacting a specific scenario. In recent years, critics have argued that threat-based planning was too restrictive to apprehend the range of expected future military engagements (Hicks, 2017). CBP emerged in an attempt to better provide a rational framework for decision making and allow plans to be more responsive to uncertainty, economic constraints, and associated risks (TCPJSAG, n.d.). Simply stated, CBP allows the development of strategies without limiting the analysis to a specific enemy or threat.

Furthermore, CBP focuses on an end goal, followed by an analysis of what needs to be done. The more information about a specific threat or scenario there is, the better military capabilities can be built. Additionally, the concept of CBP "recognizes the interdependence of systems (including materiel and people), doctrine, organization and support in delivering defense capability, and the need to be able to examine options and trade-offs among these capability elements in terms of performance, cost and risk so as to identify optimum force development investments" (TCPJSAG, n.d.). CBP "relies on scenarios to provide the context against which to measure the level of capability" (TCPJSAG, n.d.). For example, cyber capabilities include responding to crises, monitoring networks, protecting systems, testing penetration, supporting operations, and educating stakeholders. Cyber capability planning may begin with an end goal of protecting an information system, and then identify the tasks that would need to be accomplished to achieve that goal within a certain budget or utilization of resources.

According to TCPJSAG, there are several components to effective CBP. First, CBP should be output oriented, with "high-level capability objectives derived from government guidance." Second, CBP should consider "the way in which the force that is going to be used will fight," which typically comes from top-level doctrines. Third, CBP should cluster or partition groups of similar processes to make them manageable. Fourth, the resulting capabilities must be accomplished with the available resources (TCPJSAG, n.d.). These four components include the concepts of strategic, operational, and employment frequently found in militaries.

Challenges of CBP. Since CBP has been traditionally used in the military, it is integrated in the national budget and is a topic used in military readiness debates. Therefore, converting CBP from a strictly military planning strategy to one that includes civilian requirements, as is the case with cyber, presents a challenge. In the case of workforce development, it is difficult to realize the third and fourth rules from the TCPJSAG (n.d.) previously described, i.e. that CBP should partition groups of similar processes to make them manageable and that the resulting capabilities should be accomplished given the available resources. It is challenging to know the what cyber skills are needed and being produced in the civilian and military sectors. This lack of clarity creates a national challenge. Until these features are specified, it is difficult for cybersecurity training to be attuned to workforce needs (Li and Daugherty, 2015).

The major difficulty in aligning cybersecurity capability and need is a lack of a sufficient number of cybersecurity workers. The United States' best defense to emerging cyber threats is to "develop a robust, agile, and highly trained cybersecurity workforce. However, to build this workforce, organizations must have an understanding of their current supply as well as approaches to identify and meet future demand" (Department of Homeland Security, 2014). It is easy to recognize the important role that cybersecurity workers have in national defense and capability planning, however, there is a lack of cybersecurity workers in the workforce in relation to the number of positions that need to be filled. Moreover, beyond the current need for cybersecurity capabilities, even more cybersecurity workers will be needed in the future.

In February 2017, the Global Information Security Workforce Study from $(ISC)^2$ identified a workforce gap between cybersecurity workers demanded and those able to fill those rolls. The consortium projects a shortage of 1.8 million workers by the year 2022 (International Information System Security Certification Consortium, 2017). In addition, CyberSeek projects that there are, at the time of writing, 285,681 total cybersecurity job openings with a very low supply of cybersecurity workers (CyberSeek, n.d.). The scarcity of qualified cybersecurity workers is a major issue for the federal government. In 2015 the former Federal CIO (the U.S. Government's Chief Information Officer), Tony Scott estimated more than 10,000 openings for cyber workers without enough individuals to fill those positions (Ravindranath, 2015). Policymakers must address this deficit by creating a pipeline in which individuals may be first trained in cybersecurity, and then hired and retained in the government cybersecurity workforce.

The Office of Personnel Management (OPM) released a memorandum in 2016 titled *Federal Cybersecurity Workforce Strategy*. The purpose of this memo was to identify goals and desired outcomes for strategic recruitment. The memo was created to "engage in Government-wide and agency-specific efforts to conduct outreach and recruitment for cybersecurity talent and improve and expand on existing hiring and retention efforts" in order to increase the "pipeline of cybersecurity talent entering the federal workforce, including candidates who have not traditionally considered federal employment, and provide reliable and effective human resources services that enable agencies to immediately fill vacancies" (OPM, 2017). One way that this can be accomplished is through outreach to multiple stakeholders, including public, private, and academic sectors as a way to raise awareness for career paths and scholarship opportunities, such as the CyberCorps Scholarship for Service (SFS) and DoD Information Assurance Scholarship Program (IASP) (OPM, 2017).

Steps Toward Capability Planning and Workforce Development

In 2014, the Department of Homeland Security (DHS) released its first version of a cybersecurity capability maturity model, referred to as the NICE Capability Maturity Model (CMM). This capability maturity model was created to provide a framework that organizations can use as a "baseline for current capabilities in cybersecurity workforce planning" (Department of Homeland Security [DHS], 2014). This method also enables organizations to compare their capabilities to each other and give decision makers the information needed to support increased cybersecurity human capital initiatives (DHS, 2014).

The NICE CMM document is divided into three main areas: "process and analytics," "integrated governance," and "skilled practitioners and enabling technology." Process represents the activities associated with planning and building organizational processes, while analytics refers to the activities related to supply and demand data, tools, and models for workforce planning analysis. Integrated governance includes events related to establishing and developing governance structures, such as assignments of responsibility. Finally, the skilled practitioners section provides information on establishing a professional workforce and enabling technology to be used for data systems (DHS, 2014).

The NICE CMM also contains three maturity levels, ranging from the most basic level to achieving a fully developed workforce. The first level, designated "limited," addresses the start of development with limited established processes, lack of clear guidance, or few analysis methods. The second level, termed "progressing," refers to the stage in which some cybersecurity workforce planning aspects have been established and some infrastructure supports workforce planning. The final level is termed "maturity," which includes optimal cybersecurity workforce planning capability, integration with business processes, and adequate workload analysis, which together guide decision making for the cybersecurity workforce (DHS, 2014). This model can be used to evaluate the current state of the cybersecurity workforce among military branches, and then create goals to enhance the workforce and move from a "limited" level to a "maturity" level. In short, the model allows readers to understand the processes, methods, and infrastructure in place and identify the level of support that the cyber workforce is achieving. This identification can help address shortcomings and then better enable training programs, including academic programs, that prepare candidates to fulfill capability needs.

In 2009, the National Institute of Standards and Technology (NIST), along with strong leadership from DHS and the DoD, developed the NICE Cybersecurity

Workforce Framework, which can be found in NIST Special Publication (SP) 800-181 (NIST, 2017). This framework was developed as a resource to allow for a more effective method of identifying, recruiting, developing and maintaining its cybersecurity talent. This can be utilized as a foundation for the development of training standards for the cybersecurity workforce.

The NICE framework consists of seven categories of common cybersecurity functions: analyze, collect and operate, investigate, operate and maintain, oversee and govern, protect and defend, and securely provision (NIST, 2017). Each category has specialty areas that define distinct areas of cybersecurity work. Within each specialty area are identified specific knowledge, skills, and abilities (KSAs) to perform tasks in a work role. For example, in the category of operate and maintain there is a specialty area of data administration. Within data administration are the ability to maintain databases, knowledge of computer networking and privacy principles, and the skill to generate queries and reports required to complete the tasks required by a data administrator, such as analyzing and planning for changes in data capacity requirements (NIST, 2017).

The NICE framework strives to engage government, academia, and industry in an attempt to raise the proficiency and capability of information security professionals (Newhouse, Keith, Scribner, Witte, 2017). As noted earlier, cybersecurity workforce capabilities are essential to the success of capability planning. However, there remains a deficit of cybersecurity practitioners, especially in the government setting. This is concerning for national security.

Workforce Incentives. Programs such as the National Science Foundation (NSF) CyberCorps SFS and the DoD IASP should be further expanded in an attempt to meet the current and future demand of cybersecurity practitioners in the government. Both of these scholarship programs pay for students' education in cybersecurity related degrees (U.S. Office of Personnel Management, 2017). After scholarship recipients complete their education, they are required to work in a cybersecurity related field for a United States government organization. The fiscal year 2018 budget request allocates $55 million for CyberCorps SFS, with a focus on veterans (NSF, 2018). That amount of funding would allow over 2,000 students to complete the program (McAfee, 2018). Given the extent of the cybersecurity deficit, this is not enough to sufficiently decrease the workforce gap.

Another challenge facing SFS and IASP programs is the verification process. Colleges and universities that are interested in participating in SFS need to be designated by the National Security Agency and Department of Homeland Security as Centers of Academic Excellence (NSA/DHS CAE) for Cyber Defense Education

(CDE) and Cyber Operations (CO) and deemed equivalent to the certified schools (U.S. Office of Personnel Management, 2017). The NSA/DHS CAE designation process verifies that certified programs will educate students in a manner that will allow them to be successful working in a government agency. The primary goal of the CAE-CDE/CO programs is to "reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise for the Nation" (National Security Agency, 2016).

Rigorous assessments are required to certify colleges and universities. All CAE-CD institutions must have a curriculum that meets the criteria established by the NSA in conjunction with NICE and the NICE Workforce Framework (National Institute of Standards and Technology, 2017). Thus, the process of verifying schools that can then establish scholarship programs to train students for cybersecurity positions in the government is already in place, but adequate funding is required for the program to be successful.

Workforce Pipeline. For three successive presidential administrations, cybersecurity focused CAE programs have been studied, discussed, and verbally supported. Most recently, the 2016 Cybersecurity National Action Plan (CNAP) proposed that $62 million be invested in cybersecurity personnel, including strengthening the National CAE in Cybersecurity program (Office of the Press Secretary, 2016). Unfortunately, no funding lines have been created to sustain this important capability. Without funding, the existence of the CAE process, the process of validating schools for participation, and ensuring that students are properly trained may be jeopardized. Ensuring allocated funds for this purpose can help decrease the deficit of cybersecurity workers entering the government workforce. Funding is urgently needed as designated CAE schools require validation renewal and additional schools seek verification. Currently, there are 242 schools recognized with at least one CAE designation. Approximately 11,400 students graduated from CAE-CD institutions in 2017 (Centers of Academic Excellence, 2017). If more schools receive CAE certification, additional students will receive the necessary education to fill the growing number of cybersecurity job vacancies and help meet capability gaps.

K-12. Moreover elementary and high school students, should be exposed to cybersecurity topics during such a critical time in their development to help facilitate a knowledgeable population and stimulate entry into cybersecurity fields. This is especially important because training individuals who do not have any cyber skills can be costly. Instead, it is often cheaper and more efficient to build a pipeline of candidates with pre-existing skills (Li and Daugherty, 2015). One example by which early skill building can be enhanced is by expanding the use of GenCyber camps. According to GenCyber, its summer cybersecurity camps provide experiences for students and teachers at the K-12 level. The goals of GenCyber are to increase student interest in cybersecurity careers and to improve teaching methods and curricula. GenCyber has grown from eight camps in 2014 to 149 camps that will host more than 5,300 students and teachers in 2018. From 2014 to 2017, more than 10,000 students and teachers have attended GenCyber camps. Inspiring young people and encouraging them to pursue cybersecurity is an important aspect to supplying the career pipeline and increasing cyber capabilities. (GenCyber, n.d.) Funding for GenCyber was provided by the NSA and the NSF, but there is currently no Congressional funding allocated to these camps, as the program has been treated as a pilot. Without adequate funding, there is the potential that these camps will not occur. In short, there is a nationally developed program without a funding line.

Other DoD Scholarships and Camps. The DoD also offers several other STEM scholarships. These include the National Defense and Engineering Graduate Fellowship (NDSEG), the Science, Mathematics and Research for Transformation (SMART) SFS, and the Stokes Education Scholarship Program (DoD STEM, 2018).

Two other established camps aimed at fostering youth cyber education include CyberPatriot, a National Youth Cyber Education Program created by the Air Force Association (CyberPatriot, 2013) and InfraGard Cyber Camps, which are cybersecurity camps for youth offered through a partnership between the FBI and members of the private sector.

CONCLUSION

The U.S. federal government workforce lacks a sufficient number of cybersecurity workers, and given that cyber threats continue to grow, a workforce that is capable of protecting the United States' cyberspace is necessary. One potential pipeline for cybersecurity practitioners that work for the federal government currently exists, but it lacks adequate funding. Sufficient funding has the potential to bridge the gap between a currently understaffed cyber workforce and the cyber capabilities that the United States requires. Military cyber capability planning can be enhanced with the use of the NICE Framework as a basis for training, developing, and maintaining cybersecurity talent. This methodology focuses on developing a knowledgeable and skilled cybersecurity workforce. GenCyber camps and scholarship programs provide other potential sources for K-12 education and talent pools from which college students might be recruited to work for government agencies and the military, but aspects of these programs remain unfunded. To reduce the gap between the number of cybersecurity workers needed in the government setting and those currently being supplied, academia programs must be expanded and the agencies that validate CAE schools should receive adequate funding. Such actions could reduce the deficit of cybersecurity workers and enhance military cyber capabilities.

REFERENCES

Balasevicius, T. (2016). *Is it time to bring back threat-based planning?* Retrieved from http://mackenzieinstitute.com/is-it-time-to-bring-back-threat-based-planning/

Centers of Academic Excellence. (2017). *CAE in cybersecurity community*. Retrieved from https://www.caecommunity.org/

CyberPatriot. (2013). *What is CyberPatriot*? Retrieved from http://www.uscyberpatriot.org/Pages/About/What-is-CyberPatriot.aspx

CyberSeek. (n.d.). *Cybersecurity supply/demand heat map*. Retrieved from https://www.cyberseek.org/heatmap.html

Department of Defense. (2011). *Department of Defense strategy for operating in cyberspace*. Retrieved from https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

Department of Defense Science Board. (2017). *Task force on cyber deterrence*. Retrieved from https://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf

Department of Defense STEM. (2018). *STEM scholarships*. Retrieved from http://www.dodstem.us/stem-programs/scholarships

Department of Homeland Security. (2014). *Cybersecurity capability maturity model white paper*. Retrieved from https://niccs.us-cert.gov/sites/default/files/Capability%20Maturity%20Model%20White%20Paper.pdf?trackDocs=Capability%20Maturity%20Model%20White%20Paper.pdf

GenCyber. (n.d.) *About GenCyber*. Retrieved from https://www.gencyber.com/about/

Hicks, K. (2017). *Bad idea: Arguing over capabilities- vs. threat-based planning. Defense 360*. Retrieved from https://defense360.csis.org/bad-idea-arguing-capabilities-vs-threat-based-planning/

International Information System Security Certification Consortium. (2017). *Cybersecurity workforce shortage projected at 1.8 million by 2022*. Retrieved from http://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html

Li, J. & Daugherty, L. (2015). *Training cyber warriors: What can be learned from defense language training?* Santa Monica, CA: RAND Corporation.

McAfee. (2018). *Cybersecurity workforce shortage*. Retrieved from https://www.mcafee.com/us/about/public-policy/skills-shortage.aspx

National Institute of Standards and Technology (2017). *National centers of academic excellence in cyber defense*. Retrieved from https://www.nist.gov/sites/default/files/documents/2017/01/30/cae-cd.pdf

National Science Foundation. (2018). *NSF Fiscal Year 2019 budget to advance innovation, infrastructure*. Retrieved from https://www.nsf.gov/news/news_summ.jsp?cntn_id=244676

National Security Agency. (2016). *National centers of academic excellence in cyber defense*. Retrieved from https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *NIST special publication 800-181. National initiative for cybersecurity education (NICE) cybersecurity workforce framework*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

NIST (2017). *National initiative for cybersecurity education (NICE) cybersecurity workforce framework*. Retrieved from https://csrc.nist.gov/csrc/media/publications/sp/800-181/archive/2016-11-02/documents/sp800_181_draft.pdf

Office of Personnel Management. (2017). *Strategic recruitment for cybersecurity*. Retrieved from https://chcoc.gov/sites/default/files/Strategic%20Recruitment%20for%20Cybersecurity%20Model%20July%202017.pdf

Office of the Press Secretary. (2016). *Cybersecurity national action plan*. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

Ravindranath, M. (2015). *Federal CIO: More than 10,000 openings for cyber pros in the federal government*. Retrieved from http://www.nextgov.com/cio-briefing/2015/11/federal-cio-more-10000-openings-cyber-pros-federal-government/123794/

The Technical Cooperation Program Joint Systems and Analysis Group. (n.d.). *Guide to capability-based planning*. Retrieved from https://www.acq.osd.mil/ttcp/reference/docs/JSA-TP-3-CBP-Paper-Final.doc

U.S. Office of Personnel Management. (2017). *CyberCorps scholarship for service*. Retrieved from https://www.sfs.opm.gov/

Wallace, I. (2013). *The military role in national cybersecurity governance*. Retrieved from https://www.brookings.edu/opinions/the-military-role-in-national-cybersecurity-governance/