Cybersecurity for the Nation: Workforce Development

Lieutenant Colonel Karen J. Dill

ABSTRACT

Cyberspace "is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures." [1] It is the newest military domain affecting the Operating Environment (OE) and the focus of concern by the President of the United States. In the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, President Trump directed the Department of Defense and other agencies across the whole of government to identify a long-term way ahead to address education and retention of cybersecurity professionals. [2] There are two potential programs Chemical, Biological, Radiological, Nuclear (CBRN) Response Enterprise (CRE) [3] and the Civil Air Patrol (CAP), which could provide a framework that supports long-term education and retention of the US government cyber workforce.

The Problem: How to Develop a Cyber Workforce Talent Pool

The Longfellow poem of patriot Paul Revere's ride which proclaimed "One, if by land, and two, if by sea" [4] is an early acknowledgment of a warfighting domain influencing the Operating Environment (OE) that commanders considered before employing forces. The warfighting environments expanded asnew technologies provided means to strike the adversary and further national strategic objectives. The Air domain joined land and sea domains in World War I and II. Later, during the Cold War, American strategists embraced Space as a warfighting domain. Military technologies including satellite communications, electronic computers, and the Internet evolved rapidly over time and were embraced, improved, and adapted by the civilian population for widespread use to create, exchange, and store data. The civilian use of the named technologies produced what is now collectively known as "Cyberspace".

Lieutenant Colonel Karen J. Dill is an Army Signal Officer and a graduate of the Joint Command, Control, Communications, Computers and Intelligence/Cyber Staff and Operations Course (JC-4ICSOC). She served in positions as a Director of Information Management, Brigade Signal Officer, Defense Coordinating Element Operations Officer, Joint Signal Planner, and is a former Assistant Chief of Staff, G6. Currently, she is an instructor at the U.S. Army Command and General Staff College in Fort Leavenworth, KS.

The term Cyberspace does not have a standard or agreed upon definition. The Tech Terms Computer Dictionary notes that the term "cyberspace" is a popular and overused term describing the virtual world of computers.[5] Various dictionaries call it "the realm of electronic communication"[6] or "the online world of computer networks and the Internet." The Department of Defense (DoD) and Department of Homeland Security (DHS) use a more expanded cyberspace definition defining it as "A global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[7] For this article, cyberspace refers to that definition. The Cyberspace domain is the newest military OE, and a serious concern of the President of the United States.

Nationally, the use of cyberspace catapulted United States (US) growth in both government and civilian sectors making that same cyberspace a target for exploitation. Cybersecurity is "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."[8] The growth of the cyber domain continued while laws and policies to shape cybersecurity practice lagged due to a lack of knowledge gap within either a centralized government or private administration. This gap increasingly opened doors for nefarious actors to exploit vulnerabilities and resulted in multiple points of hazard to national critical infrastructure and defense systems. State, non-state, and criminal actors are actively working to leverage their cyberspace capabilities to counter US national objectives while the DoD is challenged to develop and retain an expert cyber workforce that includes a critical cybersecurity talent pool. There are existing non-cyberspace related programs from across the Armed Forces that provide frameworks for addressing the long-term development of the US cybersecurity workforce.

The Chemical, Biological, Radiological, Nuclear (CBRN) Response Enterprise (CRE) [9] and the Civil Air Patrol (CAP) are two established programs that align and professionally develop their workforce to provide a nested and multi-component approach to event response where specialized skills, knowledge, and abilities are required from private, state, and federal responders. The CRE provides an excellent model to leverage active and reserve component manpower to provide a scalable and trained response force to disasters and catastrophic events. The CRE works by delivering specialized military teams supporting a larger integrated response to a CBRN incident. The enterprise is an excellent model to investigate because as a cybersecurity response force it would provide a specialized and professional cybersecurity response at the point of need. If modeled on the CRE, a similar cyber-focused program could potentially leverage existing federal and state funding streams for training, manning, and equipping the expert teams. A lack of funding is not the only shortfall associated with a robust cybersecurity response. A significant challenge in cybersecurity is meeting continual workforce growth objectives. Apart from the CRE model, the CAP program model is a viable solution to grow and retain the overall workforce, specifically the cybersecurity workforce, which a primary concern at the highest level of government.

The White House issued the *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure on May 11th, 2017 directing cybersecurity risk management of all federal networks and infrastructure* across the whole of government and to “build and maintain a modern, secure, and more resilient executive branch [Internet Technology] architecture.” [10] The President directed four areas to be addressed for cybersecurity for the nation: Policy, Deterrence and Protection, International Cooperation, and Workforce Development.

The Problem: How to Develop a Cyber Workforce Talent PoolThe Proposal: Develop the Cybersecurity Workforce by Establishing a Civil Cyber Force Modeled After the Civil Air Patrol

The top priority of the DoD cyber strategy is to develop a Cyber Mission Force and a supporting cyber workforce through training, recruiting and retention, and private sector support. [11] A long-term cyberspace advantage can only be established if the US develops and retains a cybersecurity talent pool that is educated, dedicated, and integrated into society to protect the national cyberspace domain. The CAP is an established program that develops educated, dedicated, and integrated cadet and adult members. As a result of their training program, the CAP personnel are prepared to respond as part of a nested and multi-component approach to emergency response when specialized skills, knowledge, and abilities are required from civilians, state, and federal responders. A similar Civil Cyber Force (CCF) program could leverage youth interest in the cyberspace domain, and develop the 12 to 19-year old population of innovative, future cyber professionals as part of a military or whole of nation response to a cyberspace related crisis.

The CAP, founded in 1941, is an Auxiliary of the U.S. Air Force and retains approximately 56,000 members nationwide.[12] Participants are volunteers and Total Force[13] partners who devote their "time, energy and expertise toward the well-being of their communities. The Cadet Program is developed around five program elements: Leadership, Character Development, Aerospace Education, Physical Fitness, and Activities."[14] As a result, cadets completing the program often go into military and civilian jobs where they can make a difference and excel. Similar benefits are seen in Junior Reserve Officer Training Corps (JROTC) programs that use their "education in citizenship, leadership, social and communication skills, physical fitness and wellness, geography, and civics" to produce healthy students who have integrity and personal accountability; are actively participating in the community, society, and government; and value the role of the military and other service organizations."[15] Establishing a CCF with similar program foundational elements will embed ideas including volunteerism, commitment, service, and loyalty in the future workforce. A secondary effect of a CCF program would be a stabilized force with reduced turnover of cybersecurity professionals from the workforce. This approach meets the DoD strategic pillar to improve military and civilian recruitment and retention.

CAP program membership includes cadet youth at the program's core and active adult members who serve as mentors, trainers, and program advocates. Successful CCF recruitment would mirror the CAP program with youth as the bulk of membership, supported by active adult members. Second, CAP generates community support from other groups including Friends of CAP who help fund the program, educators who support Science, Technology, Engineering, and Math (STEM) goals of CAP, and parents who encourage their cadet CAP members. CAP cadets interact with community and business leaders and have the ability to influence community opinion and support at the grassroots level. DoD Cyber Strategy notes that "Success requires close collaboration across DoD, between agencies of the U.S. Government, with the private sector, and with US allies and partners."[16] A CCF program that leverages youth, parents, educators, and community members for support, training, mentorship, and interaction will cultivate the link to the private sector. As the CCF matures and youth move on to defense, public, or private employment many will maintain social networks established through the CCF participation and service. This will achieve the second cyber strategy pillar of developing stronger private sector support.

Last, education and training is a critical requirement of the CAP for all members. Youth attend year-round programs that test them with leadership, technology, and fitness challenges. On average, cadets spend eight hours per month plus one Saturday per month conducting CAP training, and they participate in military Service, Joint, Interagency, Intergovernmental, and Multinational exercises.[17] Adult members support the program by providing mentorship and assist in promoting the cadet program. The organization as a whole maintains a curriculum of engaging STEM topics and resources that leaders and cadets use to grow their skills. CAP cadets get special tuition rates to American Sentinel University for degrees furthering the CAP mission. There are other benefits such as discounted IT products, magazines, and travel. This highlights the requirement for education that is available to all cadets.

Education is perhaps the most challenging and critical element of establishing a CCF. The National Security Agency (NSA) outreach to STEM programs employed throughout the public school system[18] and their National Centers of Academic Excellence in Cybersecurity[19] serve as a foundation for curriculum development. Likewise, the DoD's Cyber Strategic Goal for building ready forces includes support for the National Initiative for Cyberspace Education. This comprises working with interagency partners, educational institutions, and state and private sector partners to support workforce development.[20] As the CCF program matures and cyberspace capabilities change, the curriculum, goals, nd core values can be adjusted to meet future workforce requirements.

While the NSA outreach program provides a starting point, there are multiple ongoing private national cyber education initiatives built to encourage, test, and fund cyber defense skills of elementary, high school, and college students. In fact, CAP squadrons and JROTC cyber teams routinely leverage these programs and competitions as a focus for training. CyberPatriot, Hak4Kidz, and CyberCorps®: Scholarship for Service (SFS) are some of these programs.

The Air Force Association's (AFA) CyberPatriot program which began in 2009 with a national cybersecurity completion now seeks to "to inspire K-12 students toward careers in cybersecurity or other STEM disciplines critical to our nation's future.[21] CyberPatriot links industry, government, and students in a cyber defense competition between students who try to find vulnerabilities and harden the defense of a Windows system and networks.[22] The program was well received by industry professionals and is now sponsored by multiple corporations including Northrop Grumman Foundation, Cisco, Symantec, and the University of Maryland University College. The corporate interest is a proof of concept that the private sector is willing to invest in youth cyber education programs. The CyberPatriot program participation has continuously expanded and now includes AFA Cyber camps and an Elementary School Cyber Education Initiative. Their elementary cyber education initiative meets many of the requirements proposed within the CCF including encouraging students to learn about cybersecurity careers, the importance of cybersecurity, introduces cybersecurity principles, and helps students to better protect themselves.[22]

The next generation of cybersecurity workforce and experts are today's hackers. Youth-oriented "white hat" hacking events such as the traveling Hak4Kids events or the long-running Roots Asylum use hands-on workshops, games, and simulations to improve technical and STEM skills, and enable elementary and high school students to discover the joy of ethical hacking through.[24] Unlike the CyberPatriot program where teams compete to harden a network, the Hak4Kids and Roots events use problems, puzzles, and cognitive training games to exercise an individual's STEM and logic skills to stop hackers before damage is done.[25] The Roots Asylum offers a "safe playground" for kids to explore cybersecurity, cryptography, and hardware hacking.[26] These two programs grab youth interest, hone their skills in relevant technology and software, and generate an understanding of the consequences associated with hacking. Hak4Kidz and Roots Asylum both show the benefits of hands-on cyber playgrounds. CCF curriculum could include and benefit from developing and leveraging portable cybersecurity labs and cybersecurity ranges for novices to learn about old IT infrastructure which forms the national base infrastructure, as well as experiment with new and emerging technology that will enable them to defend future cyberspace more effectively and efficiently.

Last, the CyberCorps: SFS meets the financial needs of college-age students pursuing cybersecurity and information assurance career fields. The program is a National Science Foundation scholarship opportunity for students in cybersecurity-related degree programs at nation-wide select two- and four-year colleges and universities.[27] The overarching program goal is to increase and strengthen the cadre of federal information assurance professionals protecting the government's critical information infrastructure.[28] SFS is similar to the DoD's Reserve Officer Training Corps (ROTC) 2-, 3-, and 4-year scholarship program as a path to military service where cadets incur a military service obligation as military officers, so too the SFS students fulfill a federal service obligation. The tenure is based on the scholarship length. Military junior officers meet their professional obligation by serving in Active Duty, Reserve Force, and National Guard units nationwide. In the CyberCorps SFS program, graduating students receive a merit-based scholarship, and following graduation are obligated to complete a 10-week internship followed by employment in positions in federal, state, local, or tribal governments.[29] The key difference between the SFS obligation and the ROTC obligation is that the SFS students must seek their internship and post-graduation opportunities.[30] The CCF as a hybrid organization can take advantage of the CAP program youth-base and ROTC accessions structure to produce the next generation of cybersecurity professionals. The CCF would encourage and foster youth interest, loyalty, and education in a cyber curriculum like CAP; and like the CyberCorps SFS, the CCF would funnel qualified students into senior-level scholarship opportunities at approved, degree-producing, institutions with a follow-on civil or federal service obligation.

Recommendation and Conclusion

> We live in a time of growing cyber threats to U.S. interests. State and non-state actors threaten disruptive and destructive attacks against the United States and conduct cyber-enabled theft of intellectual property to undercut the United States' technological and military advantage. We are vulnerable in cyberspace, and the scale of the cyber threat requires urgent action by leaders and organizations across the government and the private sector. [31]

The DoD is facing an enormous cyberspace challenge, and must cultivate a cybersecurity workforce to address long-term cybersecurity requirements. There are multiple defense activities that are tested and meet specialized workforce needs. They provide an adaptable framework that supports building and aligning cybersecurity professionals to protect US cyberspace, retain the advantage, and respond to a crisis. Two essential programs, CBRN Response Enterprise and CAP, demonstrate how youth and current professionals can be leveraged to draw from involved youth to meet the workforce development and retention challenges in a multi-layered environment. A variety of government and privately sponsored educational programs and events provide a ground framework to provide state-of-the-art training while laying the groundwork for the future workforce. Further research opportunities on this topic include extensive reviewing other Armed Forces youth programs such as JROTC, U.S. Coast Guard youth programs, and scouting organizations. The DoD should investigate establishing a CCF that is modeled after the CAP, and conduct preliminary appraisals of youth cybersecurity education programs, and civil-military emergency response enterprises and programs. This is an investment that America must make to meet the threats of today and prepare for the dangers of tomorrow.

NOTES

[1] Margaret Rouse, “Cyberspace,” *SearchMicroservices,* accessed May 19, 2017, http://searchmicroservices.techtarget.com/definition/cyberspace.

[2] “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” whitehouse.gov, May 11, 2017, https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

[3] Heinrich Reyes, “CBRN Response Enterprise,” March 14, 2012, accessed May 18, 2017, http://dtic.mil/ndia/2012/CBRN/Reyes.pdf, 7.

Johnny Lairsey, “The CBRN Response Enterprise in the Homeland,” *Small Wars Journal Blog,* August 1, 2012, accessed May 19, 2017, http://smallwarsjournal.com/blog/the-cbrn-response-enterprise-in-the-homeland.

[4] Henry Wadsworth Longfellow, “Paul Revere Heritage Project,” *Paul Revere's Ride,* 1869, accessed May 19, 2017. http://www.paul-revere-heritage.com/poem.html.

[5] Per Christensson, "Cyberspace Definition," TechTerms, (2006), accessed August 28, 2017. https://techterms.com/definition/cyberspace.

[6] “Cyberspace,” *Dictionary.com.* Accessed August 28, 2017, http://www.dictionary.com/browse/cyberspace.

[7] Joint Chiefs of Staff, JP 6-0, *Joint Communications System* (Washington, DC: Government Printing Office, June 2015), vii. The Department of Homeland Security definition for cyberspace is identical to the DoD joint definition.

[8] Department of Homeland Security, “National Initiative for Cybersecurity Careers and Studies,” *Glossary,* last modified August 2, 2017, accessed August 28, 2017, https://niccs.us-cert.gov/glossary#C. The DHS NICCS Portal’s cybersecurity lexicon is intended to serve the cybersecurity communities of practice and interest for both the public and private sectors.

[9] Reyes, *CBRN Response Enterprise,* 7, The CRE is U.S. Northern Command (USNORTHCOM) and National Guard Bureau multilayered organization response teams whose missions are to conduct CBRN response operations within the United States to support civil authorities in response to CBRN incidents; Johnny Lairsey, *Small Wars Journal Blog.* The CRE developed after the 1993 World Trade Center bombing under Presidential Decision Directive 39, Nunn-Lugar-Domenici Amendment 4249, National Defense Appropriations Act 2007, 2009, and 2010.

Fully established in 2012, the enterprise is a conglomeration of Title 10 units allocated to USNORTHCOM and National Guard units assigned to their respective states. The CRE consists of Weapons of Mass Destruction Civil Support Teams (WMD-CSTs), Homeland Response Forces (HRF), CBRN Enhanced Response force Packages (CERFPs), Command and Control CBRN Response Elements (C2CREs), Defense CBRN Response Force (DCRF) and Joint Task Force Civil Support.

[10] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, Sec 1 (c) (v).

[11] Department of Defense, *The Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, April, 2015), 17.

[12] Civil Air Patrol National Headquarters, *Civil Air Patrol:* About CAP, last modified 2017, accessed May 20, 2017, http://www.gocivilairpatrol.com/about/.

[13] Total Force is defined by the author as a military force including personnel from active duty, reserve component, National Guard, and auxiliary forces.

[14] Civil Air Patrol National Headquarters, *Information for Parents for Prospective Cadets,* last modified 2017, accessed May 20, 2017, http://www.gocivilairpatrol.com/cap_home/parents/.

[15] U.S. Army Cadet Command (ROTC), *The JROTC Program,* accessed May 20, 2017, https://www.usarmyjrotc.com/JROTC_information.html.

[16] Department of Defense, “The Department of Defense Cyber Strategy” (Washington, DC: Department of Defense, April, 2015), 41, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[17] Michael Marek, “Operations Exercise Success,” *Civil Air Patrol Communications Blog,* March 13, 2017, accessed on May 17, 2017, https://www.capmembers.com/emergency_services/communications-blog/?operations_exercise_success&show=entry&blogID=1827.

NOTES

[18] National Security Agency, "Resources for Educators", last modified May 3, 2016, accessed on May 21, 2017, https://www.nsa.gov/resources/educators/. NSA established various outreach programs for teachers at the K-12, undergraduate and graduate levels to engage students on the importance of science, technology, engineering and math (STEM) and language education, and to inspire future generations to consider National Security and STEM careers.

[19] National Security Agency, "Resources for Educators", last modified May 3, 2016, accessed on May 21, 2017, https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/.

[20] Department of Defense, 18.

[21] Air Force Association. "CyberPatriot." *What is CyberPatriot?.* http://www.uscyberpatriot.org/Pages/About/What-is-CyberPatriot.aspx, accessed November 13, 2017.

[22] Air Force Association. "CyberPatriot," *History.* http://www.uscyberpatriot.org/about/history, http://www.uscyberpatriot.org/about/history, accessed November 13, 2017.

[23] Air Force Association. "CyberPatriot." *What is CyberPatriot?.* http://www.uscyberpatriot.org/Pages/About/What-is-CyberPatriot.aspx, accessed November 13, 2017.

[24] Hak4Kids. "Hak4Kids," *About.* http://www.hak4kidz.com/about.html and r00tz Asylum, "r00tz Home" https://r00tz.org/, accessed December 20, 2017.

[25] Man, Jeffrey. "Hak4kidz.com in the news," video, 1:45, April 1, 2017. https://www.youtube.com/watch?v=WSdfVS6it80.

[26] Nico Sell. "Techcrunch," *"Breaking good" by teaching kids to hack at Rootz Asylum,* August 17, 2016, https://techcrunch.com/2016/08/17/breaking-good-by-teaching-kids-to-hack-at-r00tz-asylum/, accessed December 20, 2017.

[27] Department of Homeland Security, "National Initiative for Cybersecurity Careers and Studies." *CyberCorps®: Scholarship for Service (SFS)* (2017). https://niccs.us-cert.gov/formal-education/cybercorps-scholarship-service-sfs, accessed December 27, 2017.

[28] U.S. Office of Personnel Management, "CyberCorps®: Scholarship for Service", *CyberCorps®: Scholarship for Service.* (2017), https://www.sfs.opm.gov/default.aspx, accessed December 27, 2017.

[29] U.S. Office of Personnel Management, "CyberCorps®: Scholarship for Service", *Students: Frequently Asked Questions (FAQs) (2017),* https://www.sfs.opm.gov/StudFAQ.aspx, accessed December 27, 2017.

[30] Ibid.

[31] Department of Defense, 33.