JANUARY 2019

The Cybersecurity Workforce Gap

William Crumpler & James A. Lewis

As cyber threats continue to grow in sophistication, organizations face a persistent challenge in recruiting skilled cybersecurity professionals capable of protecting their systems against the threat of malicious actors. With cybercriminals now responsible for billions in losses per year and state-sponsored hacking groups posing an ever-greater threat, the need for individuals capable of securing networks against attackers has never been greater. However, education and training institutions in the United States have so far found it difficult to keep pace with the growing need for cyber talent. This paper highlights the gaps that exist in the nation's current cybersecurity education and training landscape and identifies several examples of successful programs that hold promise as models for addressing the skills gap. It then highlights recommendations for policymakers, educators, and employers.

A recent CSIS survey of IT decisionmakers across eight countries found that 82 percent of employers report a shortage of cybersecurity skills, and 71 percent believe this talent gap causes direct and measurable damage to their organizations.[1] According to CyberSeek, an initiative funded by the National Initiative for Cybersecurity Education (NICE), the United States faced a shortfall of almost 314,000 cybersecurity professionals as of January 2019.[2] To put this in context, the country's total employed cybersecurity workforce is just 716,000. According to data derived from job postings, the number of unfilled cybersecurity jobs has grown by more than 50 percent since 2015.[3] By 2022, the global cybersecurity workforce shortage has been projected to reach upwards of 1.8 million unfilled positions.[4]

Workforce shortages exist for almost every position within cybersecurity, but the most acute needs are for highly-skilled technical staff. In 2010, the CSIS report *A Human Capital Crisis in Cybersecurity* found that

[1] CSIS, *Hacking the Skills Shortage* (Santa Clara, CA: McAfee, July 2016), https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf.
[2] CyberSeek, "Cybersecurity Supply/Demand Heat Map," accessed January 4, 2019, https://www.cyberseek.org/heatmap.html.
[3] Ariha Setalvad, "Demand to fill cybersecurity jobs booming," *Peninsula Press*, March 31, 2015, http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/.
[4] Frost & Sullivan, *2017 Global Information Security Workforce Study* (2017), https://iamcybersafe.org/wp-content/uploads/2017/06/europe-gisws-report.pdf.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

the United States “not only [has] a shortage of the highly technically skilled people required to operate and support systems already deployed, but also an even more desperate shortage of people who can design secure systems, write safe computer code, and create the ever more sophisticated tools needed to prevent, detect, mitigate and reconstitute from damage due to system failures and malicious acts.”[5] At the time, interviews indicated that the United States only had about 1,000 security specialists with skills and abilities to take on these roles, compared to a need for 10,000 to 30,000 personnel.

In the nine years since that report, these challenges have persisted. In 2016, CSIS found that IT professionals still considered technical skills like intrusion detection, secure software development, and attack mitigation to be the most difficult to find skills among cybersecurity operators.[6] A 2018 survey of California businesses revealed that a lack of required technology skills was one of the greatest challenges facing organizations when hiring cybersecurity candidates.[7] These challenges were particularly acute for mission critical job roles, with over a third of organizations reporting a lack of technology skills in candidates for vulnerability assessment analyst positions and half of employers reporting deficiencies for cyber defense infrastructure support candidates.

Employers today are in critical need for more cybersecurity professionals, but they do not want more compliance officers or cybersecurity policy planners. What organizations are truly desperate for are graduates who can design secure systems, create new tools for defense, and hunt down hidden vulnerabilities in software and networks.[8]

Do Cybersecurity Graduates Possess the Skills Employers Need?

An evaluation of U.S. cybersecurity workforce development initiatives must ask whether cybersecurity education and training programs are preparing students for the kinds of high-skilled technical roles that represent the most serious workforce shortage. The evidence suggests that the answer may be no.

According to the recently published *Report to the President on Supporting the Growth and Sustainment of the Nation’s Cybersecurity Workforce*, authored by the U.S. Department of Commerce and Department of Homeland Security, “employers increasingly are concerned about the relevance of cybersecurity-related education programs in meeting the needs of their organizations.”[9] In 2016, a CSIS survey of IT employers found that only 23 percent thought education programs were fully preparing students to enter the cybersecurity industry,[10] and in 2018, professional association ISACA found that 61 percent of organizations believe that fewer than half of all applicants for open cybersecurity positions are actually qualified for the job.[11]

According to cybersecurity practitioners, employers are dissatisfied because they perceive the graduates of these programs as lacking practical experience as well as an understanding of the fundamentals of

[5] Karen Evans and Franklin Reeder, *A Human Capital Crisis in Cybersecurity* (Washington, DC: CSIS, November 2010), CSIS Commission on Cybersecurity for the 44th Presidency, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/101111_Evans_HumanCapital_Web.pdf.

[6] CSIS, *Hacking the Skills Shortage*.

[7] John Carrese et al., *Cybersecurity: Labor Market Analysis and Statewide Survey Results* (California: California Community Colleges Centers of Excellence for Labor Market Research, June 2018), http://business.ca.gov/Portals/0/Files/CASCADE/cybersecurity-labor%20market-analysis.pdf.

[8] Franklin S. Reeder and Katrina Timlin, *Recruiting and Retaining Cybersecurity Ninjas* (Washington, DC: CSIS, October 2016), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/161011_Reeder_CyberSecurityNinjas_Web.pdf.

[9] The U.S. Secretary of Commerce and the U.S. Secretary of Homeland Security, *A Report to the President on Supporting the Growth and Sustainment of the Nation’s Cybersecurity Workforce: Building the Foundation for a More Secure American Future* (Washington, DC: May 2018), https://www.nist.gov/sites/default/files/documents/2018/07/24/eo_wf_report_to_potus.pdf.

[10] Evans and Reeder, *A Human Capital Crisis in Cybersecurity*.

[11] ISACA, “State of Cybersecurity 2018 Part 1: Workforce Development,” April 17, 2018, http://www.isaca.org/Knowledge-Center/Research/Documents/cyber/state-of-cybersecurity-2018-part-1_res_eng_0418.PDF?regnum=458196.

computing and information security. As a result, many graduates require extensive on-the-job training before they can begin work. In addition, employers often find cybersecurity graduates lacking in essential soft skills like teamwork, problem-solving, and communication.[12] Organizations are also frustrated by the current cybersecurity education ecosystem, which lacks common metrics or rankings to help employers understand what programs, certifications, and degrees are the most effective. Addressing these issues would help the United States strengthen its cybersecurity talent pipeline.

MASTERING THE FUNDAMENTALS

Cybersecurity encompasses a broad range of specialty areas and work roles, and no single education program can be expected to cover all of the specialized skills and sector-specific knowledge desired by each employer. However, there are certain knowledge sets and skills that are essential for any new employee in a critical technical work role, regardless of the field they are in or the specialty they adopt. This includes an understanding of computer architecture, data, cryptography, networking, secure coding principles, and operating system internals, as well as working proficiency with Linux-based systems, fluency in low-level programming languages, and familiarity with common exploitation methods and mitigation techniques.[13] Employers are finding that graduates are lacking this foundation. One recent response from a major corporation to a request for information issued by NICE indicated that "the current [education] environment does not provide a common baseline set of skills from which to build the role specific knowledge necessary to meet employer workforce requirements."[14]

Many cybersecurity programs appear to be emphasizing cybersecurity policy planning, compliance audits, and other skills which ultimately have less impact on the security posture of an organization than the tasks enabled by a deep technical background. Studies have consistently shown that it is these tasks—including penetration testing, secure system design, incident response, and tool development—that represent the greatest need for organizations. However, these roles can only be filled by workers with a mastery of computing fundamentals and a detailed understanding of how an organization's information systems operate.[15]

Traditional computer science programs do not educate their students in the basics of information security. According to a 2016 study, only 1 of the top 36 computer science programs in the country requires a cybersecurity course for graduation, and 3 of the top 10 programs offered no cybersecurity classes at all.[16]

[12] John Costanzo, *Bridging the Cybersecurity Talent Gap in Hampton Roads* (Hampton Roads Cybersecurity Education, Workforce, and Economic Development Alliance, July 2017), http://securitybehavior.com/hrcyber/doc/HRCyber%20Mid-Project%20Report.pdf; Ray Lapena, "Survey Says: Soft Skills Highly Valued by Security Team," Tripwire, October 17, 2017, https://www.tripwire.com/state-of-security/featured/survey-says-soft-skills-highly-valued-security-team/; Arthur Conklin, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development – Request for Information Response," August 3, 2017, https://www.nist.gov/sites/default/files/documents/2017/08/03/university_of_houston_center_for_information_security_research_and_education.pdf; Sara Castellanos, "Cybersecurity Requires 'Insatiable' Problem-Solving Skills; Technical Skills Can Be Taught," *Wall Street Journal*, May 24, 2018, https://blogs.wsj.com/cio/2018/05/24/cybersecurity-requires-insatiable-problem-solving-skills-technical-skills-can-be-taught/.

[13] George I. Seffers, "National Security Agency Program Fills Critical Cyber Skills Gaps," *Signal Magazine*, June 1, 2014, https://www.afcea.org/content/national-security-agency-program-fills-critical-cyber-skills-gaps; Chris Krebs, "Why So Many Top Hackers Hail from Russia," Krebs on Security, June 22, 2017, https://krebsonsecurity.com/2017/06/why-so-many-top-hackers-hail-from-russia/; Intelligence and National Security Alliance, *Cyber Intelligence: Preparing Today's Talent for Tomorrow's Threats* (Arlington, VA: September 2015), https://www.insaonline.org/wp-content/uploads/2017/04/INSA_Cyber_Intel_PrepTalent.pdf; Workforce Intelligence Network for Southeast Michigan, *Cybersecurity Skills Gap Analysis* (Michigan: July 2017), https://winintelligence.org/wp-content/uploads/2017/07/FINAL-Cybersecurity-Skills-Gap-2017-Web-1.pdf; Laura Lee, "Circadence responses to NIST RFI on Cybersecurity workforce education or training," August 2, 2017, https://www.nist.gov/sites/default/files/documents/2017/08/02/circadence.pdf;

[14] Steve Sharkey, Drew Morin, and John Hunter, "Comments of T-Mobile USA, Inc." August 4, 2017, https://www.nist.gov/sites/default/files/documents/2017/08/04/t-mobile.pdf.

[15] Martin C. Libicki, David Senty, and Julia Pollak, *H4ackers Wanted: An Examination of the Cybersecurity Labor Market* (RAND, 2014), https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf; Homeland Security Advisory Council, *CyberSkills Task Force Report* (Washington, DC: Fall 2012), https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final_0_0.pdf; Evans and Reeder, *A Human Capital Crisis in Cybersecurity*.

[16] CloudPassage, "CloudPassage Study Finds U.S. Universities Failing in Cybersecurity Education," April 7, 2016, https://www.cloud-

Without exposure to cybersecurity practice, computer science graduates emerge facing steep barriers to entry in the cybersecurity field.

In order to meet the demand for skilled cyber operators, education and training programs must focus their curricula to ensure that students are able to achieve mastery in the fundamentals of computing and information security. Without this knowledge, graduates will find it difficult to adapt throughout their careers as threats and technologies evolve.

HANDS-ON EXPERIENCE

One of the most consistent complaints against cybersecurity education programs is that an over-emphasis on theory and book learning prevents students from building the practical skills they need.[17] Theory alone does not prepare graduates for the tasks they will face once they step onto the job. Practical training and hands-on experience is necessary to equip students with the tangible skills employers expect.

Surveys consistently show that organizations rate hands-on experience above all other factors when evaluating new hires,[18] and the integration of a hands-on learning environment where students work on realistic cybersecurity challenges has been identified as one of the key factors setting apart leading education programs in the eyes of cybersecurity practitioners.[19] The cybersecurity training nonprofit organization U.S. Cyber Challenge notes, "The common thread across the most effective public, private, domestic, or international cyber workforce training programs is hands-on, applied learning methods."[20]

Despite this, many organizations continue to find that students emerging from cybersecurity programs lack hands-on experience. According to the professional association ISACA, "Their training is also most often based in theory. They receive very little hands-on training; thus, the skill sets need to be developed on the job."[21] As a result, the very value of a cybersecurity degree has begun to decline in the eyes of employers, with surveys indicating that as many as 80 percent of hiring managers no longer believe a four-year degree adequately prepares students for cybersecurity jobs.[22]

One solution to the deficit of practical skills in cybersecurity graduates is to expand apprenticeship, internship, and work-study offerings for students.[23] These opportunities give students a chance to apply what they have learned in a real-world environment, developing tangible skills in the process and giving a grounding to the theory-based components of their education. While these opportunities serve as useful supplements to existing education programs, there are also ways for instructors to do more to incorporate hands-on learning opportunities directly within the curricula themselves. The use of cyber ranges[24] and

passage.com/company/press-releases/cloudpassage-study-finds-u-s-universities-failing-cybersecurity-education/.

[17] Conklin, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"; U.S. House Committee on Homeland Security, *Challenges of Recruiting and Retaining a Cybersecurity Work Force: Hearing before the Subcommittee on Cybersecurity and Infrastructure Protection*, 115th Cong., 1st sess. (September 7, 2017), https://docs.house.gov/meetings/HM/HM08/20170907/106359/HHRG-115-HM08-Transcript-20170907.pdf; ISACA, "Preparing Cybersecurity Professionals to Make an Impact Today and in the Future," August 1, 2017, https://www.nist.gov/sites/default/files/documents/2017/08/01/nice_rfi_final_isaca.pdf; Lee, "Circadence responses to NIST RFI on Cybersecurity workforce education or training."

[18] CSIS, *Hacking the Skills Shortage*; ISACA, "State of Cyber Security 2017: Part 1: Current Trends in Workforce Development."

[19] Ponemon Institute LLC, *2014 Best Schools for Cybersecurity* (Michigan: February 2014), https://www.ponemon.org/local/upload/file/2014%20Best%20Schools%20Report%20FINAL%202.pdf.

[20] US Cyber Challenge, "Cybersecurity Workforce RFI," August 1, 2017, https://www.nist.gov/sites/default/files/documents/2017/08/03/20170801_nist_rfi_comments_us_cyber_challenge.pdf.

[21] ISACA, "Preparing Cybersecurity Professionals to Make an Impact Today and in the Future."

[22] National Initiative for Cybersecurity Education, "Workshop on Cybersecurity Workforce Development: Notes from Panel Discussions," August 2, 2017, https://www.nist.gov/sites/default/files/documents/2017/09/28/chicago_workshop_summary_notes.pdf.

[23] Michael Prebil, "Teach Cybersecurity with Apprenticeship Instead," New America, April 14, 2017, https://www.newamerica.org/education-policy/edcentral/teach-cyber-apprenticeship-instead/.

[24] David Raymond, "Using Cyber Ranges for Cybersecurity Education," Virginia Cyber Range, https://csrc.nist.gov/CSRC/media/Events/Federal-Information-Systems-Security-Educators-As/documents/24.pdf.

cybersecurity competitions,[25] for example, has been growing in popularity among education and training providers over the past several years. These offerings give students the chance to experience challenges modeled on real-world situations, letting them build practical skills while also improving their ability to work as teams in a fast-paced, adversarial environment.[26]

SOFT SKILLS

The first priority of all cybersecurity education and training programs must be to build technical proficiency in their students. However, this does not mean that schools can ignore the need for students to develop the soft skills that can turn that technical knowledge into value for their employers. Organizations have consistently noted that soft skills like communication, teamwork, and problem-solving are crucial for new hires. One survey by the security company Tripwire found that 100 percent of respondents considered soft skills to be important when hiring for a security team, and 21 percent even went so far as to say that they were more important than hard skills.[27]

Many graduates emerge from cybersecurity education programs without these soft skills. In our survey of IT decisionmakers, CSIS found that 70 percent considered communication to be a scarce skill set among cybersecurity graduates, and more than half struggled to find candidates strong in collaboration and team leadership.[28] The failure to develop these skills has a serious impact on the effectiveness of graduates once they enter the workplace. The ability to work as a team is essential since cybersecurity is rarely handled by single individuals. Problem-solving forms the very foundation of effective cybersecurity work, and many graduates face significant obstacles troubleshooting real-world systems. Finally, communication and writing skills are essential for translating technical insight into value for a company, whether by communicating threats and trends to business management or by writing and implementing effective, user-friendly cybersecurity policies to protect an organization's information systems.[29]

Education and training programs can give students the opportunity to build these skill sets. One example is the use of cybersecurity competitions, which allow students to gain experience working as a team with others to confront realistic cybersecurity situations. These competitions, and other hands-on learning opportunities, also help students to develop analytical and problem-solving skills, which are consistently listed as among the most important soft skills by employers.[30] Finally, instructors can shift their teaching and assessment approaches to emphasize oral and written communication, for example by adopting scenario-based assessments that require students to describe their processes or respond to questions by a hypothetical business manager about how to respond to an attack.

Exemplars

In our research and discussions with leading cybersecurity practitioners, there were several cybersecurity education and training programs that were repeatedly identified as examples of how to organize and structure workforce development efforts to align with the needs of employers. By examining the approach

[25] Tim Polk, "Building the Workforce through Cybersecurity Competitions," The White House, July 27, 2016, https://obamawhitehouse.archives.gov/blog/2016/07/27/building-workforce-through-cybersecurity-competitions.

[26] Katzcy Consulting, *Cybersecurity Games: Building Tomorrow's Workforce* (Reston, VA: April 2017), https://www.nist.gov/sites/default/files/documents/2017/04/24/cyber_games-_building_future_workforce_final_1031a_lr.pdf.

[27] Ray Lapena, "Survey Says: Soft Skills Highly Valued by Security Team," Tripwire, October 17, 2017, https://www.tripwire.com/state-of-security/featured/survey-says-soft-skills-highly-valued-security-team/.

[28] CSIS, *Hacking the Skills Shortage*.

[29] Sarah K. White, "Cybersecurity skills aren't taught in college," CIO from IDG, December 13, 2016, https://www.cio.com/article/3149098/it-skills-training/cybersecurity-skills-aren-t-taught-in-college.html.

[30] Costanzo, *Bridging the cybersecurity talent gap in Hampton Roads*; Castellanos, "Cybersecurity Requires 'Insatiable' Problem-Solving Skills; Technical Skills Can Be Taught."

and operation of these programs, we can identify best practices that may assist other education and training programs to prepare their students for cybersecurity careers.

UK CYBER RETRAINING ACADEMY

The Cyber Retraining Academy is an effort by the UK government to provide an opportunity for those with high natural aptitude, but no formal cyber background, to undergo an intensive 10-week program that prepares them to transition into cybersecurity careers. The initiative, funded by the government's National Cyber Security Programme and developed in partnership with the SANS Institute, has shown promise due to its emphasis on mastering computing fundamentals and its extensive use of labs, competitions, and other hands-on teaching methods.

As many of its candidates enter the program with no background in IT, let alone cybersecurity, the academy's curriculum focuses heavily on developing students' knowledge of computing and security fundamentals. Specifically, the academy's curriculum begins with instruction on computer hardware, data structures, networking principles, information system design, and the operation of Linux and Windows-based systems.

Once students understand the fundamentals about how core information technologies work, instructors then begin to introduce them to security concepts like incident handling, exploitation methods, network forensics, and secure systems design. As the curriculum transitions to building these practical skills, the teaching methods similarly shift from theory-based learning to hands-on work. The academy uses long labs and an integrated capture-the-flag style competition to give students the opportunity to gain hands-on experience applying the concepts taught throughout the program. According to instructors, the academy begins with 75 percent theory, but transitions to 100 percent hands-on work by the end of the course.[31]

Though only two classes have graduated so far, the academy has already shown promise at producing work-ready cybersecurity professionals. The academy boasts a 100 percent placement rate of its students into industry roles after graduation, successfully turning former bartenders, journalists, and psychiatrists, for example, into cyber practitioners for the likes of Huawei, Airbus, and NATO.[32] Every company involved in the Cyber Retraining Academy's first class of graduates returned to sponsor its second cohort, indicating that the academy's approach to retraining could hold promise as a model for other initiatives hoping to quickly train work-ready talent to begin filling the cybersecurity skills gap.

CAE-CO

The National Centers of Academic Excellence (CAE) program is a U.S. government program that focuses on improving cybersecurity education in the United States by encouraging colleges with cybersecurity degrees to meet a set of academic standards developed by experts at the NSA and DHS. Today, over 230 schools have been designated as CAEs, with the majority recognized as Centers of Academic Excellence in Cyber Defense (CAE-CD), focusing on reducing vulnerabilities in our national information infrastructure. An additional 20 programs have met the more rigorous requirements necessary to be recognized as Centers of Academic Excellence in Cyber Operations (CAE-CO), concentrating on specialized offensive cyber operations to enhance U.S. national security.

Though CAE-CD schools have sometimes attracted criticism for a lack of rigor in their programs,[33] the CAE-CO program has garnered widespread praise for its emphasis on fundamental knowledge and practical

[31] Eleanor Dallaway, "All You Need to Know about the Cyber Retraining Academy," *Infosecurity Magazine*, March 31, 2017, https://www.infosecurity-magazine.com/news-features/all-you-need-cyber-retraining/.

[32] Ibid; Nick Ismail, "The Cyber Retraining Academy: training industry-ready cyber professionals," Information Age, January 24, 2017, https://www.information-age.com/cyber-retraining-academy-123464137/.

[33] Homeland Security Advisory Council, *CyberSkills Task Force Report* (Washington, DC: Fall 2012), https://www.dhs.gov/sites/de-

training. In 2012, for example, the Homeland Security Advisory Council (HSAC) Task Force on CyberSkills noted that the CAE-CO schools were the only universities in the country offering cybersecurity coursework that could "assure employers that hands-on skills are a major criterion for graduation."[34]

This emphasis was by design. The CAE-CO designation was developed by the NSA in 2012 after the agency found that graduates from the traditional CAE schools lacked the technical expertise and hands-on experience the NSA required for its workforce.[35] To understand what the CAE-CO program does differently, it is useful to look at the example of how the program approaches the subject of low-level programming. Low-level programming languages, like assembly and C, operate at the core of a computer's hardware and operating system. A familiarity with these languages is crucial for cybersecurity experts because it is at this level that most cybersecurity vulnerabilities are found and where most exploits are performed.[36] Many modern computer science programs have moved away from teaching these languages to their students, instead emphasizing high-level languages like Java, Python, or PHP that are used for building web and mobile apps.[37] Even CAE-CD schools are not required to teach their students low-level programming, including it only as an optional knowledge unit in their curriculum requirements.[38] The CAE-CO program, however, lists low-level programming as the very first of its mandatory program content and requires that students be given programming assignments that test their ability to use low-level programming concepts to implement exploits on vulnerable systems.[39]

In addition to its emphasis on fundamental knowledge, the CAE-CO program is also notable for its requirements that schools incorporate hands-on lab opportunities for multiple subjects, including software reverse engineering, networking, and cyber defense.[40] The CAE-CO program also provides opportunities for students to gain hands-on experience working with the NSA through summer internships, ensuring that every student has the chance to be exposed to real, on-the-job training over the course of their education.[41]

By requiring that schools cover basic technical skills and incorporate hands-on labs into their curriculum, the CAE-CO program has helped spur the development of many of the leading cybersecurity programs in the country and can point the way towards a superior model for university-level cybersecurity education. The United States should consider raising the standards for all CAE schools to match those of the CAE-CO program and doing more to encourage other universities to align their curricula with the CAE-CO standards.

U.S. Cyber Challenge

The U.S. Cyber Challenge (USCC) is a national program supported by DHS that develops and hosts cybersecurity camps and competitions for high school, college, and postgraduate students. The USCC

fault/files/publications/HSAC%20CyberSkills%20Report%20-%20Final_0_0.pdf; David Wennergren et al., *Increasing the Effectiveness of the Federal Role in Cybersecurity Education* (Washington, DC: National Academy of Public Administration, August 2015), https://www.napawash.org/uploads/Academy_Studies/Cyber-CAE-Report-FINAL-10-15.pdf.

[34] Homeland Security Advisory Council, *CyberSkills Task Force Report*.

[35] Upasana Gupta, "NSA Launches Cyber Operations Program," Careers Info Security, June 14, 2012, https://www.careersinfosecurity.com/nsa-launches-cyber-operations-program-a-4860.

[36] Eamon Javers, "Meet the NSA's hacker recruiter," CNBC, October 1, 2014, https://www.cnbc.com/2014/10/01/meet-the-nsas-hacker-recruiter.html.

[37] George I. Seffers, "National Security Agency Program Fills Critical Cyber Skills Gaps," *Signal Magazine*, June 1, 2014, https://www.afcea.org/content/national-security-agency-program-fills-critical-cyber-skills-gaps.

[38] National Security Agency, "CAE Requirements and Resources," https://www.iad.gov/nietp/CAERequirements.cfm.

[39] National Security Agency, "Criteria for Measurement for CAE in Cyber Operations Fundamental," https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-fundamental/requirements.shtml.

[40] Ibid.

[41] Lynne Clark and Heather Eikenberry, "Centers of Academic Excellence in Cybersecurity," National Cryptologic Schools, 2016, https://www.fbcinc.com/e/nice/presentations/2016/Track_D_Century_C/D-10_Clark_CAE_in_Cybersecurity_Programs_-_NICE_2016.pdf.

consists of two complementary initiatives: the Cyber Quests online challenge series and the week-long Cyber Camp program for aspiring cyber professionals. The Cyber Quests are a set of online challenges testing basic knowledge and aptitude in information security and cover tasks ranging from secure coding to network monitoring.[42] Based on performance in the Cyber Quests, participants are invited to one of USCC's Cyber Camps. The Cyber Camps are week-long workshops incorporating hands-on labs, hacking competitions, and instruction by leading university and industry professionals in topics like penetration testing, packet crafting, and TCP/IP warfare.[43]

Through the use of innovative hands-on challenges, the USCC has emerged as a leader in identifying and training emerging cyber scholars for roles in the cybersecurity industry. Since its inception in 2010, the USCC has become one of the most successful programs of its kind in the country, with hundreds being hosted at its Cyber Camps and thousands participating in its Cyber Quests.[44] The program was noted as a leading cybersecurity competition by the NICE-sponsored white paper "Cybersecurity Games: Building Tomorrow's Workforce"[45] and in 2016 was invited to participate in the Cybersecurity Competitions Workshop hosted by the White House Office of Science and Technology Policy.[46]

The USCC is also notable for the way it has refined its Cyber Quest challenges and Cyber Camp competitions to provide direct feedback on the aptitude of participants for critical cybersecurity roles. The USCC's competitions are the culmination of more than five years of work to identify critical cybersecurity roles and ways to train and assess students hoping to fill them. This project began in 2012 when the HSAC Task Force on CyberSkills identified 10 critical work roles essential to the defense of an organization's information systems.[47] One year later, the Council on Cybersecurity's Mission Critical Work Role Project developed a job competency model to help cybersecurity competitions align their challenges to the skills and abilities needed to take on five of those roles.[48] The project developed scenarios describing a representative set of challenges faced by individuals in those critical work roles and showed how competitions could use the tasks, methods, and tools necessary to accomplish the objectives of that scenario as a basis for designing their challenges.

The USCC is the culmination of this work, having modeled its approach to participant evaluation on this scenario-based competency model. The USCC awards participants points towards their user profile and reputation based on the competencies they exhibit, with different challenges allowing competitors to demonstrate competency for different work roles.[49] This approach not only helps focus the design of competitions towards challenges that closely relate to the real needs of employers but also helps create a model of assessment that would allow organizations to track the performance of cybersecurity students and judge which ones were best prepared to take on critical work roles after graduation.

[42] Eric Chabrow, "U.S. Cyber Challenge Seeks to Boost Number of Security Pros," Bank Info Security, September 16, 2015, https://www.bankinfosecurity.com/interviews/us-cyber-challenge-seeks-to-boost-number-security-pros-i-2915.

[43] US Cyber Challenge, "US Cyber Challenge Virginia Tech Summer Camp Schedule," https://www.cyber.vt.edu/uscc/USCC%20Camp%20Schedule.pdf.

[44] National Board of Information Security Examiners, *US Cyber Challenge Research* (Air Force Research Laboratory, February 2017), http://www.dtic.mil/dtic/tr/fulltext/u2/1027888.pdf.

[45] Katzcy Consulting, *Cybersecurity Games: Building Tomorrow's Workforce*.

[46] Polk, "Building the Workforce through Cybersecurity Competitions."

[47] Homeland Security Advisory Council, *CyberSkills Task Force Report*.

[48] Jane Lute, Deirdre Durrance, and Maurice Uenuma, "Mission Critical CyberSecurity Functions: Critical roles with the most technically sophisticated knowledge, skills and abilities for enterprise cybersecurity," Council on CyberSecurity, February 2014, http://ccs-dev.azurewebsites.net/bcms-media/Files/Download?id=df2894a5-1368-4ff7-838e-a34201036520; M. J. Assante, D. H. Tobey, and T. J. Vanderhorst Jr., "Job Competency Modelling for Critical Roles in Advanced Threat Response and Operational Security Testing," Council on Cybersecurity, 2014, http://ccs-dev.azurewebsites.net/bcms-media/Files/Download?id=560b7ac8-4ba1-4657-9358-a3420103a069.

[49] National Board of Information Security Examiners, *US Cyber Challenge Research*.

Conclusion and Recommendations

Organizations today face severe challenges recruiting the talent they need to protect their systems from cybersecurity threats. While shortages exist across the board, the greatest need is for professionals with deep technical training who are able to take on high-value roles like secure system design, tool development, and penetration testing. Currently, the U.S. system of cybersecurity training and education is failing to prepare students for these roles. Employers find graduates from many programs to be lacking in fundamental knowledge, practical experience, and critical soft skills. To improve cybersecurity education in the United States, we should look to the most successful cybersecurity workforce initiatives to identify best practices that can be adopted by other programs to help prepare students for cybersecurity careers.

The UK Cyber Retraining Academy, U.S. CAE-CO program, and U.S. Cyber Challenge are three programs that help point the way towards building a more robust pipeline for cyber talent. Together, these programs offer a set of best practices that can help providers of cybersecurity education and training in the United States better prepare their students to enter the cybersecurity workforce and help employers to manage workforce shortages and recruit the talent needed to secure their systems.

From their example, we have identified several recommendations for policymakers, educators, and employers to help address the cyber skills gap:

GOVERNMENT

- NSA and DHS should raise the eligibility criteria for CAE-CD schools based on the success of the CAE-CO program. New standards should emphasize instruction in computing fundamentals, as well as engagement with hands-on learning experiences.

- NIST's National Initiative for Cybersecurity Education (NICE) should bring together educators, employers, and cybersecurity competition providers to work towards standardizing performance measurements across cyber competitions and aligning these challenges with the NICE Cybersecurity Workforce Framework and the job competency model proposed by the Council on Cybersecurity.

- The UK Cyber Retraining Academy demonstrates the potential of short, intensive training programs to reskill workers to take on critical cybersecurity roles. Policymakers should work to support and expand similar initiatives here in the United States and create incentives for companies to institute similar internal programs for their own employees.

EDUCATORS

- Educators and those who fund them should ensure that cybersecurity curricula include a strong focus on computing fundamentals to help prepare students to take on critical technical roles.

- Instructors should work to incorporate hands-on learning opportunities like competitions, challenges, and cyber ranges into cybersecurity curricula to build practical skills in students and forge partnerships with local employers to allow students to partake in apprenticeships and internships that will expose them to the cybersecurity work environment.

- Educators should support the growth of soft skills in cybersecurity students by emphasizing team assignments throughout educational curricula and by developing approaches to teaching and assessment that stress written and verbal communication.

EMPLOYERS

- Companies should build relationships with local educators to communicate critical workforce needs and skills gaps. Improved communication between employers and learning institutions will help align the cybersecurity talent pipeline with the needs of industry.
- Companies should hire cybersecurity applicants with non-traditional backgrounds—like those graduating from short-term, intensive cyber reskilling programs—as a way to fill critical workforce needs.
- Organizations should consider establishing internal retraining programs to draw from existing talent pools to fill workforce shortages.

William Crumpler *is a research assistant with the Technology Policy Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.* ***James A. Lewis*** *is a senior vice president and director at the CSIS Technology Policy Program.*

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).