
# Cybersecurity Talent Identification and Assessment

*January 2019*

CISA
CYBER+INFRASTRUCTURE


# Cybersecurity Talent Identification and Assessment

Table of Contents

# I. Introduction

It is widely reported that there is a lack of skilled cybersecurity professionals available to fill vacant positions. This information stems directly from industry-insider studies and surveys. For instance, the "2018 Cybersecurity Workforce Study" from the International Information System Security Certification Consortium (ISC)² estimates a global shortage of nearly 3 million cybersecurity professionals. Also noteworthy within the study is that 63% of the 1,452 participants reported shortages of cybersecurity staff within their own organizations. Furthermore, most of the respondents believe these workforce deficiencies place their companies at moderate-to-extreme risk of cybersecurity attacks.[1]

These observations continue trends observed in the cybersecurity news site, Dark Reading's, 2017 report, "Surviving the IT Security Skills Shortage," where 86% of the 400 Information Technology (IT) and security professionals surveyed believed there were not enough skilled security professionals available to meet market demands. This same study noted that 77% of IT managers do not believe their teams are properly trained to combat the latest security threats.[2]

In the Information Systems Audit and Control Association (ISACA) "State of Cybersecurity 2018 Report," 59% of the 2,366 participants communicated they had unfilled cybersecurity/information security positions within their organizations. Although additional report data suggested an increase in qualified candidates from the previous year, only 12% of the respondents felt they had found "well qualified applicants" for their openings.[3]

The findings from these surveys and numerous others highlight one of the biggest challenges facing organizations today; although there is a tremendous demand for cybersecurity talent, qualified candidates are not applying for open positions. Those applicants are either difficult to find, already employed, or simply do not exist. Another hypothesis is that good candidates are indeed available, but their skills and experience do not match what job recruiters are looking for. They may even possess traits that would allow them to learn and excel within cybersecurity positions, but they do not have the right criteria listed on a resume to make it past the initial screening process.

This paper, sponsored by the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security, and authored by the Software Engineering Institute at Carnegie Mellon, will explore how cybersecurity talent is currently identified. It also highlights several current and future assessment capabilities that could be leveraged to find ideal applicants for vacant information security positions. Finally, recommendations will be provided to aid in candidate identification and talent evaluation.

# II. Cybersecurity Talent Identification

While at the DEF CON cybersecurity convention in 2015, a high-ranking Department of Homeland Security official opened his speech with a challenge to attendees. If they could make his cellular telephone ring during his talk, a government job would be available to them.[4] Although this may seem a bit bold and daring, it certainly opens the door to any candidate that

could perform a specific task, within a defined period of time. The ambiguity regarding pedigree and qualifications are removed from the equation. If the objective could be met, a reward was available. Unfortunately, the cybersecurity application selection and screening processes are not always this clear cut.

There are other instances when the government has turned to the hacker community for help. In 2010, Albert Gonzalez was sentenced to 20 years in prison for stealing as many as 170 million credit card numbers; but only after he received more than $75,000 a year working undercover for the U.S. Secret Service.[5] Other notorious hackers, like Kevin Mitnick, have inspired Hollywood movies and gone on to very successful cybersecurity consulting careers, even after being convicted of wire fraud and other crimes.[6] The ideal cybersecurity path does NOT include breaking laws, with hopes to gain notoriety, and parlay that into business opportunities.

Although these examples seem a bit extreme, they are really not far-fetched. In fact, according to Monster.com, banking executives are scouting for talent at industry conferences like Black Hat, and even hosting their own ethical hacking competitions. They are combining the non-conventional, with traditional recruitment methods, collegiate partnerships, and sponsored cybersecurity camps, to help find and prepare candidates for cyber careers.[7]

Job recruiters have their own set of challenges. The biggest of which is the limited adoption of a standard cybersecurity framework or common lexicon. Although the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework) exists, most organizations do not map their open positions to the Work Roles or Specialty Areas, which it defines. Automated search tools are improving, but recruiters must often perform passive searches on sites like LinkedIn, DICE, or Indeed because the language used in cybersecurity job descriptions may differ from that outlined on candidate resumes.

Broadly speaking, a candidate cybersecurity professional's knowledge can be assessed using many of the industry certifications available. However, recruiters, employers, aspiring professionals, and academic institutions are challenged to identify which of these programs are best suited for their specific needs. Without considering specific IT venders and their related product certifications, today's top certification agencies include CompTIA, (ISC)², the SANS Institute, EC-Council, and ISACA. Each of these certification bodies boasts over 135,000 members (or certificates achieved), with CompTIA's total being over two million. With the exception of ISACA, each organization provides more than 10 different certifications. Global Information Assurance Certification (GIAC) has more than 35!

With so many different cybersecurity certifications, an ecosystem has been created that can over-value one particular program, or devalue another. For example, the Department of Defense (DoD) requires personnel performing Information Assurance (IA) functions to obtain an industry certification appropriate for their Technical (IAT) or Managerial (IAM) position, and level (I, II, or III). Twenty-eight unique certifications are identified within their Cyber Workforce Management Program (DoDD 8140.01 & DoD 8570.01-m).[8] An IAT Level I individual must earn one of four approved certifications. In this scenario, the (ISC)² Systems Security Certified Practitioner (SSCP) is weighted the same as CompTIA's Network+ credential. Although some

overlapping knowledge areas exist, there are still numerous disparities between those two certifications' objectives. Without additional specificity tied to job responsibilities, there is an increased risk for misalignment between organizational needs and employee capabilities. When possible, cybersecurity positions must have more granular, and consistent knowledge, skills, and abilities (KSAs) defined. Subsequently, these can be compared to learning objectives for industry certifications, which in turn establishes greater value when identifying job requirements.

Of the numerous cybersecurity certifications available, very few include any form of "hands-on" skills assessment. Technical certifications like the Offensive Security Certified Professional (OSCP) require students to pass a hands-on practical exam in order to obtain the certification.[9] Cisco's expert-level credential, Cisco Certified Internetwork Expert (CCIE) requires passing both a written exam and a rigorous practical exam that costs $1,600 per attempt.[10] Similarly, The GIAC Security Expert (GSE) certification from the Global Information Assurance Certification (GIAC) combines both a multiple-choice exam along with a hands-on lab portion. The GSE lab fee is over $2,400 U.S. Dollars.[11]

Cybersecurity talent identification can be challenging. Formal degrees in Computer Science or Cybersecurity, along with industry certifications can be used as a starting point. Unfortunately, these are often just point-in-time knowledge tests, and do not evaluate the individual's skills or potential. The use of non-standard terminology also makes it difficult to appropriately match candidates for an organization's needs. With the adoption of a standard lexicon, including cyber role responsibilities, education providers could better shape their curriculum to match workforce needs and help prepare students for careers in cyber.

# III. Cybersecurity Talent Cultivation

Given the challenges for finding cybersecurity talent, an effective course of action is to develop young professionals with the necessary competencies to meet the increasing demand. Following are several examples of programs supporting that objective.

The U.S. Cyber Challenge (USCC)[12] is a program supported by the Department of Homeland Security (DHS) through a contract with the Center for Internet Security (CIS). It aims to find America's best and brightest aspiring cybersecurity professionals, and consists of several components including Cyber Quests, Cyber Camps, and virtual community, CyberCompEx.

- Cyber Quests are a series of online competitions where participants demonstrate their knowledge in a variety of cybersecurity areas. Multiple events are held throughout the year.
- To attend the USCC Cyber Camp, prospective participants must receive an invitation through competing in a qualifying Cyber Quest event. The weeklong Cyber Camp programs culminate with capture the flag (CTF) competitions and award ceremonies. While at the camp, a job fair is held where attendees can meet USCC sponsors and discuss employment opportunities.
- CyberCompEx is an online collaboration of industry professionals, mentors, job seekers, and employers, and includes links to cyber competitions and other resources, with the goal of cultivating a cyber workforce through virtual networking.

Cyber challenges and competitions have existed for many years and are great experience builders, and enable organizations in industry, academia, and government, to seek out top talent amongst a large pool of potential candidates. Besides technical skills, these competitions can also highlight strengths in soft skills such as communication, team work, and comprehension of the business aspects of cybersecurity. A NICE subgroup found that cyber competitions and challenges may help alleviate the shortage in skilled employees in the cybersecurity and IT fields by reaching students at a younger age and generating an interest in a field that may have otherwise gone unexplored[13]. The committee suggests that cyber competitions need not only be used as an extracurricular activity for interested students, but also as a method for developing the workforce by improving the talent of the work pool now, instead of waiting the 5-10 years it might take for a middle or high school aged students to prepare to enter the workforce. Employers in organizations of every sector would benefit from recruiting candidates that participate in competitions, to grow their pool of skilled workers.

A few examples of cyber challenges and competitions include:

Carnegie Mellon's picoCTF[14] is a free computer security game targeted at middle and high school students. With prizes up to $5,000, the game consists of a series of challenges centered around a unique storyline where participants must reverse engineer, break, hack, decrypt, or whatever is necessary to solve the challenge.

CyberPatriot[15] is a competition held by The Center for Infrastructure Assurance and Security (CIAS) aimed at middle school and high school aged students. During the CyberPatriot competition, four teams are tasked as IT professionals responsible for assessing and hardening the cybersecurity vulnerabilities of a small network, while also maintaining availability of critical services. Teams compete by state or region, with winners advancing to the national competition for school recognition and scholarships.
The CIAS also holds the National Collegiate Cyber Defense Competition (NCCDC)[16] each year for undergraduate and graduate students from Universities across the country. The NCCDC requires teams to take a much more defensive stand, by protecting critical services and infrastructure from live attacks through detecting and responding to attack events and business requests simultaneously. Teams are scored automatically and winners receive school recognition, as well as a trophy and an excellent experience addition for their resume.
The CyberCorps® Scholarship for Service Program (SFS)[17] is a scholarship program funded through grants awarded by the National Science Foundation. The program began in 2001. Since then, it has graduated approximately 3,000 students. Recipients can receive up to 3 years of academic support, to include tuition, book expenses, and a monthly stipend while actively attending classes. In return, students agree to work in a cybersecurity role at an approved government agency or organization, for a duration equal to their scholarship period. Currently, over 70 academic institutions participate in the SFS program.

Organizations such as $(ISC)^2$, ISACA, and the Information Systems Security Association (ISSA) have scholarship programs for undergraduate and graduate students. $(ISC)^2$ has been highly successful in offering the majority of its scholarships to females and international students, a contributing effort for increasing diversity in the cyber workforce[18]. Local $(ISC)^2$ chapters, including Pittsburgh's, offer individual scholarships to local students and $(ISC)^2$ members. The

ISSA has a foundation that has awarded more than 1,000 scholarships over its 30-year existence totaling more than $3 million[19]. While membership in one of these chapters has its benefits for individuals, employers could look to them for candidate referrals, including scholarship recipients.

The private industry has taken similar steps by offering scholarship programs to attract potential candidates, and in turn strengthen their information and cybersecurity workforce. For example, CrowdStrike, a cybersecurity technology company, established the CrowdStrike Foundation to support the next generation of talent in cybersecurity. The foundation offers four scholarships annually for students studying in the field at the undergraduate or graduate level. Cisco took a slightly different approach in 2016 by providing $10 million worth of Cisco CCNA Cyber Ops training and certification scholarships to aspiring cybersecurity professionals.[20]

The state of Maryland, in conjunction with the SANS institute and funding from the Maryland Department of Labor Licensing and Regulation Earn Program, created the Cyber Fast Track program. This initiative provides a step-by-step path for individuals beginning with the cultivation of career interest, and ending with a position in the cybersecurity field. Candidates assess their natural talent through more than 250 challenges, progress through coursework at their own pace, complete core skills training through SANS (on a possible scholarship), and finally interview with multiple companies within the state of Maryland for available positions.[21]

It is crucial that organizations tie into these programs in order to access this growing resource pool. The accomplishments achieved within these programs often come with valuable experience that can be readily applied in the work environment.

# IV. Need for Performance-Based Assessment

In 1984 Universal Pictures released, "The Last Starfighter," in which the protagonist, Alex, sets the high score in the arcade game "Starfighter." Shortly thereafter, he is recruited to put his superior skills to use in an intergalactic space conflict. Although the movie plot still seems far-fetched in 2018, the concept of using an assessment tool (e.g., video game) to identify top talent for critical missions does not.

USAF Lt Col Kristal L. M. Alfonso authored a paper in 2010 recommending a similar concept. The creation of a Cyber Proving Ground (CPG) system could potentially identify the next cyber genius.[22] Using virtual worlds like the site Second Life, which was launched in 2003, participants could interact with other users, each with different skills, on separate missions, representing different agencies, and each with varying objectives. CPGs facilitate diversity of thought and provide opportunities for free-range discovery and innovation. With the highly competitive market for top talent, and the ever-evolving world of cybersecurity threats, CPGs could potentially provide both the training ground and assessment mechanism needed to identify top talent.

Carnegie Mellon's Software Engineering Institute (SEI) created a prototype of this kind of cross-domain training and assessment solution, in 2017. Combined arms training involving both cyber and kinetic operators, was executed using a combination of the SEI's Simulation, Training, and

Exercise Platform (STEP), and Bohemia Interactive's Virtual Battlespace simulator. In these scenarios, cyber operators had to defend key cyber terrain, while compromising enemy systems to provide a kinetic battlefield advantage.[23] This, and similar capabilities, provide cyber operators the opportunity to directly observe what success and/or failure look like based on their ability to perform their assigned tasks.

Other cyber assessment efforts are underway internationally. Cyber Security Challenge UK provides a series of national competitions, learning programs, and networking initiatives designed to identify, inspire, and support cybersecurity professionals.[24] The British intelligence agency – Government Communications Headquarters (GCHQ) has even launched a virtual game within Cyber Security Challenge UK in an effort to find and recruit talented hackers. Players are called upon to protect a fictional company from a group of cybercriminals using secure code analysis skills.[25] Dozens of other games exist within the freely available system, and cybersecurity topics, which include ciphers, attack strategies, vulnerability assessment, forensic analysis, and others. This national initiative also strives to introduce appropriately skilled individuals to prospective employers.

There is a plethora of cyber ranges and training capabilities available today. However, the reoccurring challenge is how to assess an individual's skills, and not just their knowledge of cybersecurity concepts. Furthermore, that validation must be tied to specific organizational needs. And hopefully, those requirements are aligned with a cybersecurity standard like the NICE Framework. Beyond these baseline capabilities, solutions must also be flexible enough to incorporate dynamic threats, changing networks, and new mission sets. To maximize return on investment, cyber assessment tools must be easy to access and cost effective enough to scale to fit each organization.

# V. Cyber Assessment Examples

Many organizations offer assessments to test soft skills like aptitude, error detection, reasoning, writing skills, or management skills. For example, IBM offers a Commercial Cyber Aptitude Test (CCAT)[26] and a Defensive Cyber Aptitude Test (DCAT)[27]. A professional's aptitude for an IT or IT security career in general, may also be assessed, but not specific to a single job role and not hands-on in nature. For example, SANS offers a CyberTalent Aptitude Assessment on comprehension, problem solving skills, and knowledge application. Leveraging training labs is another option, but very few offer hands-on assessments of technical skills. CYBRScore, for example, is one of the few assessment tools available that provides hands-on skills assessments via an on-demand environment. Following is a closer look at CCAT, DCAT, CyberTalent, CyberScore, and several others.

IBM's Commercial CCAT and DCAT exams focus on selecting, training, and retaining the right candidates for entry level Security Operations Center (SOC) analyst roles, and other IT security work roles. Either aptitude test can be administered to new hires or those in career transitions. Both exams measure the soft skills, but further, they assess behavioral traits and cognitive aptitude required to gain technical abilities. Meaning, rather than identifying an individual's existing cyber skills, it gauges the potential of the individual to develop these talents and be

successful in a cyber career. The goal of the IBM CCAT and DCAT is to make workforce growth more efficient by being able to identify individuals with the highest potential for success, and focus training and retention efforts.

SANS CyberTalent[28] is an aptitude assessment on comprehension, problem solving skills, and knowledge application. Quiz questions may include topics such as networking, mathematics, or programming, and security procedures. After completing the assessment, the user receives a summary report of strengths and weaknesses, as well as their rank among other test takers. Employers or businesses can use these results to model their own assessments based on their needs to fill candidate positions. Specific skill exams include:

- Cyber Defense
- Penetration Testing
- Application Security
- Digital Forensics
- Information Security Aptitude

The Armed Services Vocational Aptitude Battery (ASVAB) is a timed, multi-aptitude test maintained by the DoD.[29] The ASVAB Career Exploration Program (CEP) version covers eight subjects including General Science (GS), Word Knowledge (WK), Mathematics Knowledge (MK), Auto and Shop Information (AS), Mechanical Comprehension (MC), Arithmetic Reasoning (AR), Paragraph Comprehension (PC), Electronics Information (EI), and Assembling Objects (AO). Beyond its use for identifying military candidates, High School students throughout the nation use the CEP to discover strengths and career interests. In 2008, the Air Force developed the Cyber Test (CT) component of the ASVAB with consultation from all U.S. services and other subject matter experts.[30] While the test is available to applicants, it is only required for certain military occupational specialties. Incorporating the CT component into the CEP would be a tremendous step for exposing young adults to cybersecurity. In preparation for the ASVAB, the CT would provide at least some exposure to concepts such as computer networking, communications protocols, security and compliance, software programming, and PC configuration.

In 2015, the University of Maryland's Center for Advanced Study of Language (CASL) began working on a Cyber Aptitude and Talent Assessment for the U.S. Air Force (USAF-CATA). Unlike the CT, the USAF-CATA does not measure cyber knowledge. Instead, this test focuses on critical thinking, working memory, special visualization and other traits that could be predictors of high performing cyber warfare operations.[31]

CYBRScore[32] is one of the few assessment tools incorporating hands-on skills assessments through an on-demand environment. Available labs include a wide range of cyber concepts from basic firewall configuration, to incident analysis, and coding. CYBRScore's grading and scoring component interacts with lab systems to monitor changes, responses, and actions performed and inputted by the user. The scores are measured against predetermined assessment metrics designed by an instructor or developer.

ISACA Cybersecurity Nexus (CSX) platform was launched in 2017.[33] This training and certification program contains a variety of cyber courses and hands-on labs for individuals or the enterprise. CSX has several resources geared towards preparation for the CSX Practitioner (CSXP) exam. The CSXP certification is a performance-based exam involving live cyber incidents, which successful candidates must demonstrate their ability to detect and mitigate. The two-hour assessment is designed to evaluate competency in the common security functions. The cost for utilization of training and labs in this system, may prove cost prohibitive for most individuals or enterprises. Access to a course for an individual ranges from $200-$400 for a duration of 120 days to six months.

The U.S. Air Force has its own implementation for skill requirements and assessment. A training pipeline has been created for their cyber warfare operators, which includes a list of required KSAs for each unique job role within the cyber realm, at each proficiency level: apprentice, journeyman, and craftsman. Most of the technical and knowledge-based competency building is via either an Air Force course or industry certification, while practical skills are observed using an over-the-shoulder "check ride" evaluation. If the over-the-shoulder evaluations could be measured by an evaluation tool or assessment mechanism that automated scoring a candidates' performance, it would reduce the number of personnel required in the validation process, and improve the efficiency, accuracy, standardization, and pace at which service members can be qualified for their specific job and skill level.

To advance the state of this practice, the Software Engineering Institute (SEI) Cyber Workforce Development (CWD) team created performance-based assessments to evaluate and train Air Force and cyber warfare operators on a variety of cybersecurity topics and tools. Objectives and tasks are tied to the NIST Cyber Security Framework (NIST CSF) under the five core functions: Identify, Protect, Detect, Respond, and Recover. Assessment results are immediately available to students, with options to retake and/or retrain on any missed topics. Innovative techniques are used, leveraging numerous in-game variables to provide unique answers with each execution. The same tasks, conditions, and standards are trained and assessed, without the concern of answer sharing among students. This also provides repeatable training capabilities, as the hands-on lab can be taken numerous times without answers being anticipated by the student. Grading and scores are calculated using both traditional quiz engines and automated verifications built into each assessment, which are designed interrogate systems within the virtual environment. A minimum passing score is required to receive credit for completing each hands-on exercise, and students have the opportunity to view reports that detail their results on each training/assessment objective.

The DHS Risk and Vulnerability Assessment Qualification Program (DRQP) includes an SEI developed cybersecurity course along with a Culminating Training Exercise (CTE) performed in a virtual environment. Students perform a penetration test and must then detail their process and techniques in a written report to be graded by a subject matter expert. Skills and knowledge checks compare closely to the Offensive Security Certified Professional (OSCP) certification requirements, while also incorporating the SEI's Remote Vulnerability Assessments (RVA) procedures.

Other assessments explored were the Information Security Aptitude Assessment, Cyber Defense Assessment, and CyberTalent Enhanced. The former contained very basic information regarding computer security knowledge checks for the basic user, or low-level IT position.

The Cyber Defense Aptitude assessment and CyberTalent Enhanced tests were geared towards advanced cybersecurity topics, and seemed comprehensive while touching on technical topics at a more in-depth level. At a price of 25 assessments per $3,750 - $5,000, scalability becomes an issue when trying to assess a large-scale work force.

This section reviewed several cyber skill assessment tools and techniques, each with a specific goal, or target audience. A combination of two or more may be required to truly predict an individual's success in a job role. Likewise, professional achievements would be more insightful if tied to required job tasks. This highlights the value in clearly detailed and defined KSAs required for a cybersecurity work role, along with a mapping to how 'measures of success' for each can be demonstrated.

# VI. Conclusion

As many as 82% of companies utilize some type of pre-employment assessment, with as many as 54% using a form of job scenario driven simulation, for potential hires.[34] Due to the nature of the cybersecurity field, designing a one-size-fits-all evaluator is simply not feasible. Instead, evaluation and assessment tools based on a widely agreed upon framework of standards that could be applied to a number of work roles and job responsibilities, would be more beneficial.

Until the cybersecurity community adopts standardized schema to validate an individual's skillset, existing options will have to do for considering a candidate. Industry certifications and higher education degrees are still good mechanisms for identifying at least a basic level of cybersecurity knowledge, especially for those applying for a job with little to no previous work experience. A generalized aptitude test is a useful tool to gain insight into how well a candidate is suited for the cybersecurity or information technology workforce. A more specialized aptitude test that looked for the baseline behavioral traits and abilities that are indicators for high potential, are better suited for considering skills in specific work roles such as forensic analyst or penetration tester. However, reassurance of qualifications for these roles would require additional knowledge earned through continued training or certification processes. Roles which absolutely require previous IT or cybersecurity experience, would call for a targeted skills test for candidates in order for employers to have confidence in abilities.

For work roles that have high technical demands, such as digital investigations, incident response, secure coding, or penetration testing, it is crucial that the candidates are able to demonstrate they possess the technical knowledge and skills needed to be effective in their work role. A hands-on practical evaluation is the best fit in this scenario. Ideally, the hands-on assessment has objectives tied to an industry standard, like the NICE Framework. When mapped to a framework, the tool can validate qualifications by assessing successful performance against defined KSAs for that job, and potentially strengths in another work role through KSAs they may have in common. A generalized assessment, spanning across KSA's, the tester, and their

employer, would have indicators for which job role category their prominent skills and abilities align to. This could aid with job role placement, longer tenure, and increased satisfaction from candidates and transitioning employees, because of the clear indicators of position potentials and professional growth goals.

A tool that maps evaluation or assessment metrics to a known set of KSAs offers transparency. The required KSAs for open positions will seamlessly map to work roles, and produce more accurate job postings. Candidates can reference the framework to determine if they have the core skillsets identified for specific job roles prior to applying for a position. Recruiters can help find better fits for positions and refer only the most qualified candidates, as well as help guide candidates to positions where their attributes best line up with skillset requirements.

Historically, organizations were laser focused on their own success and ventures that directly, and perhaps solely, benefited them. While that was the nature of the beast, cybersecurity is a global, ubiquitously connected, concern for all. Banks, academia, industry, government, and military systems, all share the same cyber space. Cybersecurity concerns of one entity, are typically shared by others. As cybersecurity, and to a higher degree, national security, is everyone's responsibility, a cyber evaluation tool mapped to accepted standards and metrics, is most effective if it's nationally available. Not only will it foster a broad community assessing cyber workforce skills on the same scale, the tool can evolve and improve with requirements and feedback from several different perspectives.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.



DM19-0027

[1] *Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens*. (ISC)2. 2018. https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx

[2] Chickowski, Ericka. Surviving the IT Security Skills Shortage. *Dark Reading Reports*. 2017. http://cybersecurity.arcticwolf.com/rs/840-OSQ-661/images/AWN_DarkReading_Report-IT-Security-Skills-Shortage_2017.pdf

[3] State of Cybersecurity 2018. *Cybersecurity Nexus Program Overview*. December 2018 [accessed]. https://cybersecurity.isaca.org/state-of-cybersecurity

[4] Peterson, Andrea. How the government tries to recruit hackers on their own turf. *The Washington Post*. October 24, 2015. https://www.washingtonpost.com/news/the-switch/wp/2015/10/24/how-the-government-tries-to-recruit-hackers-on-their-own-turf

[5] Zetter, Kim. Secret Service Paid TJX Hacker $75,000 a Year. *Wired*. 22 March, 2010. https://www.wired.com/2010/03/gonzalez-salary/

[6] Greenberg, Andy. Kevin Mitnick, once the world's most wanted hacker, is now selling zero-day exploits. *Wired*. September 24, 2014.

[7] Felicetti, Kristen. You'll never guess which industry is now hiring hackers. *Monster*. December 2018 [accessed]. https://www.monster.com/career-advice/article/banks-courting-hacker-cybersecurity-talent

[8] DoD Approved 8570 Baseline Certifications. *IASE Information Assurance Support Environment*. December 2018 [accessed]. https://iase.disa.mil/iawip/Pages/iabaseline.aspx

[9] Offensive Security Certified Professional (OSCP) Overview. *Offensive Security*. December 2018 [accessed]. https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/

[10] CCIE - Book Your Exam. *The Cisco Learning Network*. December 2018 [accessed]. https://learningnetwork.cisco.com/community/certifications/ccie-book-your-exam

[11] GIAC Security Expert (GSE) Certification. *GIAC Certifications*. December 2018 [accessed]. https://www.giac.org/certification/security-expert-gse

[12] U.S. Cyber Challenge. *Center for Internet Security (CIS)*. December 2018 [accessed]. https://www.uscyberchallenge.org/

[13] Katzcy Consulting. *Cybersecurity Games: Building Tomorrow's Workforce*. Katzcy Consulting. 2016. https://www.nist.gov/sites/default/files/documents/2017/04/24/cyber_games-_building_future_workforce_final_1031a_lr.pdf

[14] picoCTF. *Carnegie Mellon University*. December 2018 [accessed]. https://picoctf.com

[15] CyberPatriot the National Youth Cyber Education Program. *Air Force Association*. December 2018 [accessed]. https://www.uscyberpatriot.org/home

[16] National Collegiate Cyber Defense Competition. December 2018 [accessed]. https://www.nationalccdc.org/

[17] CyberCorps. History Overview. *CyberCorps: Scholarship for Service*. December 2018 [accessed]. https://www.sfs.opm.gov/Overview-History.aspx

[18] ISC$^2$. Scholarship Opportunities with (ISC$^2$) and the Center for Cyber Security and Education. ISC$^2$ Blog. 1 March, 2018. https://blog.isc2.org/isc2_blog/2018/03/scholarship-opportunities-with-isc%C2%B2-and-the-center-for-cyber-safety-and-education.html

[19] ISSA Foundation. Scholarships. *ISSA Foundation: Investing in Tomorrow*. December 2018 [accessed]. https://issafoundation.org/scholarships/

[20] CISCO. Expand Your Career Opportunities. Cisco. December 2018 [accessed]. https://mkto.cisco.com/security-scholarship

[21] SANS. Cyber Fast Track Maryland. December 2018 [accessed]. https://cyber-fast-track.io

[22] Alfonso, Kristal. A Cyber Proving Ground: The Search for Cyber Genius. *Air and Space Power Journal*. Spring 2010. p61-66. https://apps.dtic.mil/dtic/tr/fulltext/u2/a595976.pdf

[23] Guttman, Rotem. Combined Arms Cyber-Kinetic Operator Training. SEI Blog. 20 March, 2017. https://insights.sei.cmu.edu/sei_blog/2017/03/combined-arms-cyber-kinetic-operator-training.html

[24] Cyber Security Challenge UK. Competitions. *Cyber Security Challenge UK*. December 2018 [accessed]. https://www.cybersecuritychallenge.org.uk/competitions

[25] Sparkes, Matthew. Spy agency GCHQ organizes game to spot new recruits. *The Telegraph*. 21 August, 2014. https://www.telegraph.co.uk/technology/internet-security/11046649/Spy-agency-GCHQ-organises-game-to-spot-new-recruits.html

[26] IBM. Commercial Cyber Aptitude Test (CCAT). Talent Management Solutions Data Sheet. March 2018. https://www.ibm.com/talent-management/hr-solutions/cyber-security-skills-assessment

[27] IBM. Commercial Cyber Aptitude Test (DCAT). Talent Management Solutions Data Sheet. March 2018. https://www.ibm.com/talent-management/hr-solutions/cyber-security-skills-assessment

[28] SANS. SANS CyberTalent. *Cybersecurity Workforce Programs*. December 2018 [accessed]. https://www.sans.org/cybertalent

[29] Today's Military. ASVAB Tests. *Today's Military*. December 2018 [accessed]. https://www.todaysmilitary.com/joining/asvab-test

[30] Canali, Kristophor et. al. "Cyber Selection Test Research Effort for U.S. Army New Accessions." 12 October, 2017. PowerPoint file. https://apps.dtic.mil/dtic/tr/fulltext/u2/1044605.pdf

[31] Campbell, Susan. Assessing Aptitude for Cyber Operations: Identifying potential candidates for the U.S. Air Force. *CASL Research Fact Sheet*. August 2016. https://www.casl.umd.edu/wp-content/uploads/2017/04/DO0080_FactSheet_082016.pdf

[32] CybrScore. Skills Assessment. *CYBRScore*. December 2018 [accessed]. https://cybrscore.io/assessment.

[33] ISACA. ISACA Launches Real-time, Real-world Cyber Security Training Platform and Assessment Tool. *ISACA*. December 2018 [accessed]. http://www.isaca.org/About-ISACA/Press-room/News-Releases/2017/Pages/ISACA-Launches-Real-time-Real-world-Cyber-Security-Training-Platform-and-Assessment-Tool.aspx

[34] Talent Board. 2017 Talent Board North American Candidate Experience Research Report. Talent Board. 2018.