CYBERSECURITY GAMES: BUILDING TOMORROW'S WORKFORCE

Monica Ricci and Jessica Gulick

PROLOGUE

Cyber competitions are venues, both physical and online, where participants perform in closed environments to defend the assets of an Information Technology (IT) network. Like any competition, cyber competitions are both instructional and gratifying for its participants. Within the National Initiative for Cybersecurity Education (NICE) of the National Institute for Standards and Technology (NIST), the Competitions subgroup (NICEWG) set an objective in early 2016 to explore the concepts, design strategies, and pursue actions that advance the role that competitions play in cybersecurity education, training, and workforce development.

To explore and capture the concepts behind competitions and envision how they might be expanded, 29 stakeholders with significant knowledge and experience in both competitions and cybersecurity were interviewed. Among the diverse opinions offered by the contributors, a consensus emerged: the current and projected workforce needs must be met not only by training more cybersecurity personnel, but also by raising the bar on their skills, aptitude, and ability to collaborate. Cybersecurity competitions can play a critical role in this mandate: in raising awareness, developing skills, and supplying the expanding workforce needs of organizations of every type – private and public, large, and small – to effectively defend themselves against cyber threats.

Stakeholders interviewed for this discussion

included representatives involved in cybersecurity and cyber competitions from the Department of Homeland Security (DHS), the NSA, NIST NICE, CyberPatriot, Raytheon, Northrop Grumman, BAE Systems, Leidos, the MITRE Corporation, GE, BT, the University of Maryland, University of Texas San Antonio, California State Polytechnic University, Accenture, the SANS Institute, (ISC)[2], FireEye, CyberCompEx.org, Facebook, Katzcy Consulting, Women's Society of Cyberjutsu, Lifejourney, Sherman Consulting, Zeneth Tech Partners, Ninjajobs, and Secure Decisions.

INTRODUCTION

Whether hacking critical infrastructure like utilities and financial institutions, disrupting political campaigns, stealing intellectual property, or robbing citizens of their identities and sense of security, cyber attacks increasingly threaten industries, government agencies, and both the public and private lives of individuals. The 2016 Verizon Data Breach Incident Report catalogued over 100,000 incidents and 3,141 confirmed breaches, up from 79,790 incidents (>25% increase year over year) and 2,122 confirmed breaches the previous year (48% increase year over year)[1]. To defend the nation, its industries and its citizens against existing and emerging threats, the US National Security Strategy is predicated on expanding the skilled workforce to perform duties relating to information security.

Of concern is the shortage between the number of workers with cybersecurity defense skills and the number of

[1] 2016 Data Breach Investigations Report, VERIZON (2016), http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

open job requisitions, in both private enterprise and government. The federal government faces the greatest challenge with 83% of hiring managers struggling to find and employ qualified candidates.[2] For commercial enterprises, a skilled workforce is imperative; yet experts forecast a demand for 6 million cyber workers by 2019 and a shortfall of 1.5 million.[3]

To produce this paper, the NIST NICE Subcommittee for Competitions interviewed more than 25 thought leaders from government agencies, defense contractors, other private industry entities and academia. All participants are actively engaged in cybersecurity. They shared their perspectives on this looming issue and the role that cyber competitions might play in raising awareness, enhancing education, attracting capable resources to the field, and addressing the skills gap. The interviews sought to understand:

- How effective are current competitions at all levels — secondary, university and professional — at developing and demonstrating skills, generating awareness and a pipeline of current and future professionals in the cyber defense field?
- What are the challenges and opportunities for expanding competitions beyond current levels to

---

[2] Martin C. Libicki, David Senty & Julia Pollak, *H4CKER5 WANTED: An Examination of the Cybersecurity Labor Market*, RAND (2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf, at 28.

[3] Steve Morgan, *Cybersecurity job market to suffer severe workforce shortage*, CSO ONLINE (Jul. 28, 2016), http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html.

reach larger audiences, generate more skilled resources, and elevate the skill levels of the cyber defenders in the workplace?

- Who might take the lead in elevating the scope of competitions across government, academia and private industry?

Competition stakeholders expressed diverse and sometimes contrasting opinions about the priorities in each of the above areas. Their experiences fuel numerous debates:

- Are technical skills or soft skills more important in producing a strong cyber defense?
- Does skilled cyber defense require individual or group effort?
- Should cyber training and competitions emphasize offense, defense, or both?
- Does the responsibility for addressing the workforce shortage and skills gap fall primarily to public agencies or private industry?
- How should investments in education prioritize between short-term and long-term workforce requirements?
- When does standardization of the competition and education process enable scale, and when does it hinder the creativity and agility needed in a rapidly shifting area?

Competitions, both as games or as skills development tools — could be improved through standardization and through expanding the competitive arena. Standardization could slow the pace of growth; however, if left to develop organically, competitions may not

address the growing needs of the cyber workforce in either the short or the long term.

Among the diverse opinions expressed, one core belief was shared by virtually every stakeholder: the cyber workforce shortage is so critical that it demands an artificial injection, an impetus, to attract greater interest and participation that will accelerate skills development. The arena of cyber competitions can serve as a significant contributor. Cyber gaming appeals to younger generations, representing both immediate and future cyber workforces. An organized collaboration among key stakeholders can:

- Raise public awareness of the world of cyber competition.
- Exponentially multiply the number of cyber games, sponsors, and participants.
- Inform and restructure academic curricula.
- Transform and popularize specific cyber training strategies.
- Aid recruiters in identifying talent.

Cyber competitions are believed to be highly effective in skills development by providing hands-on experience in simulated, real-world situations. What makes these competitions unique is that the social and gaming aspects of the playing field incentivize participants to be at their most innovative and productive.

When discussing the standardization of cyber competitions, interviewees frequently made comparisons to sports. To the uninitiated, cyber competitions, seem nothing like sports. There are few cyber stadiums,[4] few superstar

[4] The National Cyber League is an example where stadium-like environments have been created. *National Cyber League*,

players with recognizable names and faces beyond this specific realm,[5] no cheerleaders, no endorsement contracts, and no standard rules of the game. Yet, the essence of competition is the same: participants strive to be the best, to excel by recognizing and focusing their talents and to develop winning strategies. Professionalizing cyber competitions can mirror the structure used by large sports leagues that have achieved breadth and scale: those have rules, team roles, organized games, audiences and fans, awards, marketing, and funding through sponsorships and advertisers. The main difference between cyber and athletic competitions underscores the importance of this white paper: a real-world cyber arena exists, where bad actors with malicious intent are inflicting damage upon individuals, corporations, and nations.

- For students, competitions are held at the middle school, high school and collegiate levels and complement classroom teaching and laboratory assignments with hands-on work in a social/gaming environment that fosters learning in entirely different ways. Parents, teachers, and other mentors introduce children to the competitions so that students will hone their abilities, learn teamwork, and have fun while exploring avenues for applying their talents in the future.
- For cyber professionals in the private sector, competitions develop and demonstrate skills, evaluate the abilities of a job candidate, raise awareness among a business leaders, and boost morale and productivity.

---

https://www.nationalcyberleague.org.

[5] We acknowledge that cyber competition superstars do exist today.

- For industry and certification bodies, competitions are increasingly accepted as work experience that qualifies for recertification.
- For governments, competitions generate skills needed to defend the nation, its industries, and its citizens against the growing cyber threat. Competitions complement tabletop war games used in training. Cyber threats are a growing focus of national policy and regulation around the world. Investments encourage collaboration among all stakeholders to develop and expand the workforce, and to that end, there are a growing number of cyber competitions where nations compete against each other to develop a workforce, and to demonstrate skills and share knowledge (e.g., at the EC-Council's Hacker Halted).
- And for the cybersecurity field in general, competitions foster innovation: innovation in tactics and techniques, both offensive and defensive, where learning is shared and drives the advancement of processes, technology, knowledge, and skills among the competitors.

The contributors' opinions, case studies and anecdotes captured demonstrate that cybersecurity competitions raise awareness, develop, and demonstrate skills, and expand the pool of human resources recruited into government or private sector jobs. The social and gaming aspects are seen as particularly compelling for up-and-coming generations of potential workers, and the stakeholders participating in this white paper yearn for cyber

competitions to achieve what sports leagues have with publicity, followership, sponsorship, and participation. They wonder how all aspects of an athletic league, like baseball or football, could be adapted and utilized to both accelerate and broaden the adoption of cyber competitions. This paper makes recommendations on not only continuing but also fast-tracking this discussion, and expanding it to include all interested parties.

I. COMPETITIONS: AN OVERVIEW

The history of cyber competitions spans more than two decades. Mr. Jeff Moss, the founder of DEFCON, created the inaugural event in 1993 to bring together knowledgeable BBS (bulletin board system) hackers to speak, practice and share hacking skills.[6] Shortly after, this initiative attracted participation from industry and law enforcement in the hopes of developing better cyber defensive tactics and strategies.

Cyber competitions today come in a few different flavors. Many are events where individuals or teams play defense or offense to protect or attack assets in an Internet-connected computer network, or to solve forensic or other cyber-related challenges.

- "Capture the Flag" (CTF) competitions can involve Jeopardy-style questions or hands-on offensive-defensive activity on a network.[7]

---

[6] Helpnetsecurity, *The Story of DEFCON*, YOUTUBE (Jul. 30, 2007), https://www.youtube.com/watch?v=lg6bQMTjHCE.

[7] Tim Harmon, *Cyber Security Capture The Flag (CTF): What Is It?,* CISCO (Sept. 14, 2016), http://blogs.cisco.com/perspectives/cyber-security-capture-the-flag-ctf-what-is-it.

- In a Jeopardy-style CTF, teams are scored and advance by answering questions on topics in various cyber categories including cryptography, steganography, physical security, forensics, and scanning.
- In offensive-defensive CTF, while battling competitors, players endeavor simultaneously or alternately to defend their assets and infiltrate their opponents' network to assets to reach their objective.
- Operational competitions evaluate teams and award points not only in the technical areas of defending a network and maintaining continual service, but also in business challenges related to an IT security job function (e.g., researching technology or presenting to management). In these types of competitions, a "red team" of expert volunteers perform as hackers, and attempt to break into the network and disrupt service.
- Forensics competitions task students to solve forensic challenges either in a standalone event[8] or as part of a larger cyber competition.
- A research paper competition sponsored by the "National Security Agency Science and Security Program" recognizes the best scientific cybersecurity paper from the previous calendar year published in a peer review journal or presented at a conference. Described by Dr. Adam Tagert,

[8] *Cyber Forensic Challenge,* https://cyberforensicschallenge.com/.

director: for four years, this initiative has recognized researchers who have demonstrated lasting impact to the science of cybersecurity. The competition promotes the validity of their research and encourages more quality research in this field.

- Policy cyber competitions, such as the Atlantic Council's Cyber 9/12 Student Challenge, provide an opportunity for students across academic disciplines to interact and compete to achieve a deeper understanding of the policy challenges associated with cyber crisis and conflict. Using an interactive learning experience with a competitive scenario, exercise teams respond to a realistic, evolving cyber attack and analyze the threat it poses to national, international, and private sector interests.

Competitions may be executed in controlled environments[9] under the supervision of cyber experts from academia, government and private industry who construct the playing field ecosystem, design the scenarios, and usually act as the attackers and role play characters during the simulation to best approximate real-world business, government, and strategic situations.

Competitions can be conducted entirely online, but the most common type of competition discussed by our stakeholders is a team competition, played in rounds, in live environments where competitors, organizers, judges, educators, and sponsors are present. Most competitions score competitors as teams, but a limited few also score

[9] H. RES. 1244, *Recognizing the National Collegiate Cyber Defense Competition for its now five-year effort to promote cyber security curriculum in institutions of higher learning*, (June 29, 2010), *available at* https://www.govtrack.us/congress/bills/111/hres1244/text

individual contributions.

Competitions come from many sources: the brainchild of a single individual or the work of a large, organized group. Their operating budgets are either self-funded or financed by corporate sponsors and government grants.

II. A BRIEF INVENTORY OF COMPETITIONS

Over the course of over 25 interviews for this paper, stakeholders described their involvement with and the operation of many competitions at the secondary school, collegiate and professional level. Sixteen competitions and competitive platforms were discussed by one or more interviewees. Day-Con X, DEFCON, BlackHat and SANS NetWars are examples of professional competitions. CSAW, the National Collegiate Cyber Defense Competition (NCCDC) and the National Cyber League are examples of collegiate competitions. CyberPatriot, GE's GhostRed and the Cyber 9 ½ Challenge are examples of high school competitions. These are just a few examples. At least 38 competitions across all levels are included in common inventories. CyberCompEx.org maintains a list of active and archived competitions in the USA.

III. WHY COMPETITIONS?

Sporting metaphors are frequently used to inform everyday discussions on topics from business to education to politics. With terms like "Monday morning quarterbacking," "knocked it out of the park," and "full court press," the language of athletic competitions has bled into the lexicon of everyday life.

The conflicts within a competition make for great storytelling. Tension and interest are created as athletes and spectators eagerly await the outcome of the contests, equally ready to laud the winners and criticize the losers. There's a common desire to prevail and learn from the contests, uncovering the reasons behind a defeat and understanding the strategies that led to a win.

Professional sports are fed by an extensive structure of leagues where plays are introduced to, learn and perfect their skills. Youth leagues, such as those for baseball, football, or soccer, introduce young children to the game, and they learn fundamental skills, strategies and teamwork required to compete more effectively at higher levels. Competitions held at the middle school, high school and collegiate levels provide further opportunities for individuals to get involved, allowing thousands of young adults to try their hand at these sports and for fans of all ages to engage as they cheer on their hometown favorites. The professional leagues and their championship games are at the pinnacle of these competitive ladders. And the professional championships have large viewership, attracting sponsors who pay premium rates for advertising to those audiences.

Cyber competitions tap into the tradition of pitting one side against the other. Youth competitions offer participants a chance to learn the fundamentals of cybersecurity in a fun, engaging format and provide an entry point into the professional workforce.

"On the playing field, as in the Security Operations Center, skills matter," says Jessica Gulick, CEO, KATZCY Consulting. "But trust, communication and teamwork matter more. Cyber sports teach security professionals to think critically and creatively about offense and defense, about the measures and counter-measures associated with every move."

The NICEWG contributors believe that cyber competitions are a valuable learning opportunity for participants, regardless of skill level. "Cyber as a sport" is a growing trend in high schools; the number of high school teams that participated in the Air Force Association's CyberPatriot doubled in a two-year period from over 2,200 in 2014 to over 4,000 in 2016.[10] Educators increasingly recognize cyber competitions demonstrate and develop planning, leadership, collaboration, and communication skills and offer a compelling alternative for students of all ages who are less likely to compete or excel at physical sports.

Competitions also provide safety, security, and enjoyment. When practicing both offensive and defensive maneuvers in a typical competition environment, players are encouraged to practice and hone cybersecurity skills in a controlled, real-world environment where no harm can come to the competitors. Finally, cyber competitions are a forum for networking, team building, and information sharing.

IV. THE MANY FACES OF CYBER COMPETITIONS

In today's advanced societies, many youth have never experienced a world without computers, cellphones, and other Internet-enabled devices. And whether they enjoy Candy Crush Saga or multiplayer games, according to one estimate, the average "21-year-old has spent 10,000 hours gaming – about the same amount of time he's spent in school

[10] The number of teams registered in 2016 has reached record levels, as reflected in Cyberpatriot IX Registered Teams, AIR FORCE ASSOC., http://www.uscyberpatriot.org/Documents/CPIX%20Current%20Registered%20Teams.pdf.

from 5th to 12th grade."[11]

The social and gaming aspects are attractive to younger generations, making cyber competitions a valuable tool in recruitment and workforce development. The need to expand the cyber security workforce is behind considering how standardization and professionalization can accelerate the growth of cyber competitions in terms of number, size, reach and stature? The stakeholder community is at odds over how best to address the cybersecurity workforce shortage. As cyber competitions grow and evolve around the world in an effort to keep pace with market changes, their relative novelty and expanding adoption create a study of contrasts. The following sections describe key topics where our cyber competition experts held differing opinions on cybersecurity, competitions, and the way forward for each.

This paper's contributors listed many skills than can be developed through cyber competitions. Leadership, teamwork, and communication were most frequently cited. Increased self-confidence was another important benefit.

"The teams who perform well assign roles to team members. One member might focus on firewall and intrusion detection systems. One person might build operating systems and harden them... But frankly, we're looking for leadership: who is leading, motivating, helping them overcome when they're ready to quit, because they've been hacked." – Joseph Krull, Security Principal Director, Accenture.

Communication is essential "to make very compelling arguments as to why certain issues are important, and to determine who can identify consequences, who can

[11] Nick Shore, *Millennials Are Playing With You*, HARV. BUS. REV. (Dec. 12, 2011), https://hbr.org/2011/12/millennials-are-playing-with-y.

make decisions for prioritization and the like." – Greg Touhill, Deputy Assistant Secretary, Cybersecurity and Communications, Department of Homeland Security (DHS).

Competition builds "self-driven research skills — in these competitions. You've got to have the initiative and go out and look for things…find out how to use an exploit to help the team… or run a command. Ultimately, it's a confidence builder." – Lisa Jiggetts, CEO, Women's Society of Cyberjutsu.

V. TECHNICAL SKILLS VS. SOFT SKILLS

This paper's stakeholders believe that skills development is a critical outcome of cyber competitions. Many contributors cited the importance of teamwork and soft skills as much as they emphasized technical skills improvement. Many believe that cyber competitors and workforce professionals benefit most from technical training. Computer science and computer engineering are often cited as the most desired majors for college students being recruited into the cybersecurity workforce. Competitors and cybersecurity professionals alike must have at least a basic knowledge of "how things work," including networks, threats, and malware. Technical emphasis corresponds to the predominance of computer science and computer engineering students at cyber competitions.

But the soft skills of leadership, communication (translating technical subjects into business terms), critical/analytic thinking, teamwork, and creativity were frequently identified as desirable characteristics in a cybersecurity role. Several competition observers described team formation, team dynamics, leadership and collaborative problem-solving as characteristics in high

demand. Recruiters prefer these traits and sponsors regularly offer jobs to competitors, often during the competitions themselves.

The workforce requires both technical and soft skills, and these diverse needs are reflected in the NICE Framework and in certification organizations. As $(ISC)^2$'s Dan Waddell, regional managing director for the North America region, observes "If you put [all certification bodies] in one room and map our certifications to the NICE Framework, it covers the gamut. It covers hard-core technical skills, but also softer leadership/managerial skills, as well. You need a blend."

Although, says Laurin Buchanan, principal investigator at Secure Decisions, "[Competitions remain] focused on high school and college level students, who may or may not be studying computer science and computer engineering – which, from my point of view, is entirely useless to hire someone as a cybersecurity engineer. They don't understand networks; they don't understand threats and malware."

Contributors note that both technical and soft skills are on display during a cyber competition. Rodney Petersen, director of NICE, notes: "When I walk around the competitions and observe, I quickly notice the teamwork and how small groups of people are working together. I pick up on non-verbal behavior, leadership skills. From monitoring the activity, you can ascertain someone's technical proficiency, and then their speaking ability, as it comes up in the competition. And employers can do the same thing by walking around and observing them."

Cyber education is regularly associated with STEM (or STEAM) education (science, technology, engineering, art, and math). Whether this association helps or harms the goal of strengthening and expanding cyber skills education

is unclear. Linking cyber education to STEM may not adequately support the development of soft skills. The historical concern that sparked an emphasis on STEM education was the USA's declining rank on the global stage when it came to technology skills. The current impetus – to defend our nation, our industries, and our citizens -is more critical because of the intensifying threat. Therefore, cyber education must be addressed and deployed more rapidly and more widely than STEM.

VI. INDIVIDUAL VS. TEAM SKILLS (AND MIXED-GENDER TEAMS)

The stakeholders express different and contradictory opinions about the role of the individual versus the role of the team in cyber competitions and, more broadly, within the cyber workforce.

In hiring an employee, the individual is typically evaluated as an individual, and subsequently progresses through his or her career in the same fashion. But modern cybersecurity professionals are expected to contribute as a team. The soft skills of teamwork and knowledge of the larger business environment were cited as frequently by contributors as individual technical skills.

"There are no lone eagles; this is a team sport." – Greg Touhill, Deputy Assistant Secretary, Cybersecurity and Communications, DHS.

One of our contributors posited that the image of a white knight or the lone cyber warrior may be conjured by Hollywood (as seen, for example, in the television program *NCIS*). However, other contributors were quick to point out that security training and certification programs focused on the individual could reinforce the notion of being an army of

one. In contrast, Mike Cameron, director of business development at Leidos, reminds us, "If you look at the cyber competitions, the ability to succeed is driven not just by individual skills, but how well they communicate as a team to deploy those software skills and team behaviors and function. You're not just training, but you're doing workforce development: you are developing teams as well as people."

In the face of the forecasted skills shortage, developing and testing team skills in real-world scenarios is imperative. Evaluating individual skills and overcoming challenges of scoring (discussed later in this paper), stem from the inherent nature of cybersecurity, requiring both individual warriors and well-coordinated teams.

A note on gender and education: one contributor relayed a particularly poignant anecdote about high-school-aged girls who participated in an all-girls robotics competition. Upon completion, the young women were invited to participate in a cyber competition and were asked to choose between a mixed-gender competition and an all-girls competition. One responded that if she had been asked before the robot program, she would have chosen to be on a team with all girls. But now that the team had proven what they could do, they had confidence and would choose to be in a mixed group.

Women are gaining ground in the cyber arena, including in competitions; 2016's Brigham Young University team at the National Secretary, Cybersecurity and Collegiate Cyber Defense Competition (NCCDC) notably included four female members.[12] Stakeholders believe that

[12] Valentina Zaraya, *How These Mormon Women Became Some of the Best Cybersecurity Hackers in the U.S.*, FORTUNE (Apr. 27, 2016), http://fortune.com/2016/04/27/mormon-women-cybersecurity/.

targeted outreach to girls and women, and a focus on teamwork and soft skills that are often evident there, are necessary considerations for expanding the cyber competition and workforce arena.

VII. OFFENSE VS. DEFENSE

One of the most debated subjects among stakeholders is whether cyber education and cyber competitions should include the study of offensive skills: the role of the attacker or hacker. Most of the contributors who organize and/or sponsor secondary school and collegiate competitions believe that the scope of the game should be limited to defensive capabilities.

In the era of WikiLeaks and state-sponsored hacking, some stakeholders feel it is too much to expect competitions to teach the complex ethical issues of hacking alongside the technical and soft skills required of a cybersecurity practitioner. And there is a lingering bias that practicing offensive skills encourages the wrong talents.

This stance, however, runs counter to the beliefs of stakeholders who consider the cyber arena to be a battleground. In warfare, understanding offensive techniques is as critical as pitting might against might. As cyber threats become increasingly sophisticated, the need to "get into the enemy's mind" intensifies. This requires, they believe, expanding the study and practice of offensive methods.

"Being able to look at your defensive position as an attacker, through an attacker's eyes, is critical," says Pete Clay, principal of Zeneth Technology Partners. "From my background, a military point of view, my ability to attack has informed my ability to defend. The teams should switch

sides; the team that attacks should be on the blue side and defend in the next scenario. The ultimate goal is not just to teach a tactic, which has limited applications in the market. But teaching the tactic and then the defensive techniques to stop bad things from happening, teaching how to orchestrate and use the defenders' tools to prevent bad things from happen[ing] - this is critical."

There are pragmatic reasons for allowing competitors to play both sides. Jenn Henley, director of security at Facebook, points out, "If you've learned something in a book, by the time you've graduated and put it in practice, threat actors and models have changed. Where these competitions are so valuable – they force students to use critical thinking, take foundational skills and put them in practice. It allows them to practice both offensive and defensive [techniques]. Forces them to think as an attacker and a defender. And you can't get that from a book, or in a classroom."

"Playing a part on the blue team in information security can, to a very small degree, be compared to the lot of a hapless soldier. The soldier is told to guard a certain hill and to keep it at all costs. However, he is not told who his enemy may be, what they look like, where they are coming from, or when (or how) they are likely to strike. To ride this analogous horse a bit further, the soldier is given a hand-me-down rifle with only a few rounds of ammunition to fulfill his task. It seems a bit unfair really; even the American Revolution got Paul Revere." -- Verizon's 2016 Breach Investigations Report[13].

VIII. PRIVATE VS. PUBLIC

[13] VERIZON, *supra* note 1.

Not surprisingly, during their interviews, many interviewees made an association between patriotism and cybersecurity. In fact, today's cyber competitions draw significant investment and attention from the military services and defense industry. Mike Cameron points out, "The cyber competition community is usually at the nexus of government organizations, academia and professional organizations like the Air Force Association and others."

Public sector funds, in the form of sponsorships, have jump-started competitions, stimulated interest and awareness and increase participation. The most significant backers of some of the largest competitions, like CyberPatriot and NCCDC, are defense-related organizations or government agencies: the Armed Forces Association, DHS, NSA, Northrop Grumman, and Raytheon, to name just a few.

Yet, because 95% of US critical infrastructure is in the hands of private industry, it is private industry that has the most to gain in developing a skilled cyber workforce.. In competitions that have scaled dramatically, like CyberPatriot and CCDC, most of their funding is private rather than public.

Private industry has a growing need for highly skilled cyber employees. To create a labor supply that can meet this demand, most companies will require a business case for investment. That investment strategy may include:

- Sponsoring competitions to increase size and scope, and to expand outreach to students/competitors.
- Providing cyber expertise to competition organizers, helping them develop scenarios, offering staff as coaches and mentors, and staffing the red/white teams, etc.

- Developing technology to enable competitions to scale, working to develop standard taxonomy and process.
- Raising awareness in their communities and among their clientele – and the public in general – about the subject of cybersecurity.

Return on Investment (ROI) is important in the commercial decision-making process. Making a cybersecurity business case must quantify the impact of investing in defensive skills. Business cases must consider several items that are difficult to quantify:

- The effectiveness of marketing to increase brand awareness.
- The goodwill generated by associating with the education sector on a topic of critical importance to national defense.
- Investment in and availability of a large pool of highly-trained resources at a fair price point.

"The US Cyber Challenge focuses on the national level, to elevate the defense of our companies, governments and institutions and citizens and ensure their private and personal information doesn't get into the hands of people who will use it in a malicious way." – Karen Evans, KE&T Partners, CyberCompEx.org.

This paper's contributors generally believe that scale results when the private sector gets involved. Government seed-funding can introduce new technology; expansion, adoption, and maturity of that technology results from private investment. In the long run, for cyber competitions, the contributors all agree that the needs and involvement of private industry will ultimately elevate the game to the

benefit of private and public enterprises alike. This factor reinforces the importance of ongoing conversations and collaborations among all cybersecurity stakeholders.

IX. SHORT-TERM VS. LONG-TERM WORKFORCE NEEDS

"I tell people; if you want to be a security professional and want to wear a suit and tie every day, there is a place for you. If you want to have purple hair and sit in a corner and not talk to anyone, there's a place for you too." – Jenn Henley, Director of Security, Facebook.

When discussing the role that competitions play in secondary and higher education, and in preparing competitors for careers in cybersecurity, it becomes apparent that there are different needs and expectations in the short term versus the long term.

- Over 1.5 million cybersecurity jobs will be unfilled in the US by 2020.[14]
- A leading Internet-based company reported to the NICE Working Group that thousands of candidates apply for every open software engineering position posted; yet due to the scarcity of skilled personnel, it takes 8-12 months to hire one cybersecurity professional (in an environment with 125 open requisitions).

Re-designing the education system to create a

[14] Justin Hofherr, *All those scary hacks are creating a lot of demand for certain computer experts*, BOSTON.COM (Dec. 8, 2016), http://www.boston.com/jobs/jobs-news/2015/12/08/all-those-scary-hacks-are-creating-a-lot-of-demand-for-certain-computer-experts.

cybersecurity workforce will generate results in the long run. The stakeholders frequently compared this educational transformation STEM, noting that the approach produces results but the required pace is more urgent this time. "I remember when we were doing this for electrical engineers in the 1980s. We had a 'war for talent' long before the term was coined," says Jim Michaud, Director, CyberTalent Solutions, The SANS Institute. "In every case, the demand got met; universities changed their curriculum to educate more people; practical/tactical organizations like SANS began to do it; pay in the field was so much more that people shifted. In every other case, sooner or later, it got met."

To address the immediate and short-term demand, most agree that other tactics are required. Tactics might include:

- Raising awareness of the need to attract skilled personnel to the field, and not necessarily technically-trained people. As Laurin Buchanan says, "If you've found a problem, but you cannot communicate to your manager/CIO/CEO the potential meaning and impact, then having found it will do no good. I find that many technically-skilled people are not very good at communicating in plain language, in simple easy-to-understand terms, what is going on."
- Expanding professional competitions to develop skills and redeploy resources where they are needed. This opportunity benefits people who are re-entering the workforce or changing careers mid-stream; and based on the statistics cited above, the cybersecurity field represents a "growth industry", while other traditional job functions are on the decline.

- Creating training programs to address the need at a national level, and consider options for engaging a diverse workforce, including training women and veterans, and offering flexible working conditions. Jim Michaud notes that Alan Paller, president of SANS, makes an analogy between the deficit of InfoSec professionals and the risk to the world and the deficit of pilots before WWII. He points out that, "You do not go to a four-year university in order to learn how to fly an airplane … you go to a flight school. A lot of SANS courses and competitions are like flight schools. Before WWII, we needed 20 times the number of pilots, and we set up 22 flight schools around the country."
- Generating interest and enthusiasm among people with the skills, knowledge, or aptitude, to fill cyber positions. To target young people, make cyber "cool" and accessible. For career-age people, increase cyber-awareness and education in 'mainstream' courses of study (e.g., top MBA programs). As Jim Michaud comments, "HR professionals have learned from STEM that if we generate interest and awareness early, we can ultimately increase people in the field. In cyber, that's important, but not enough, and will take too long. Our view is, converting people mid-career from other fields through assessment tools and taking them through our program is important in the short run. Middle schoolers don't have careers for

10 years, and we need to address the problem NOW."

X. WORKFORCE DEVELOPMENT VS. EXTRACURRICULAR ACTIVITY

Student competitions are typically extracurricular activities for students. In the workforce, competitions are professional development tools. Most of the stakeholder input focused on raising cybersecurity awareness in schools as a subject to study, a skill set to develop and as a career to pursue. Workforce development, for those already in the professional arena, is an extension of the earlier debate about the short-term and long-term skills need. Increasing student cybersecurity involvement is an important long-term strategy, but there are significant short-term needs to be addressed. While there is a growing arena for professional competitions, if these are going to be accepted as tools to train and develop practitioners in the field, then stakes have to be higher than professional bragging rights.

In his IEEE paper, Dr. Gregory White, Director for Infrastructure Assurance and Security at the University of Texas, references Microsoft's Senior Technology Officer Lewis Shepherd's 2010[15] webcast, *Hiring the Next Generation of Cyber Professionals in Government*. White explains the concern that government agencies, like DHS and NSA, were hiring virtually all the available qualified professionals, leaving private industry to scramble. Foreshadowing today's crisis, Shepherd asked, "How do we train and retrain, and do 'long training,' with our current generation of professionals?"

[15]O'Reilly, Hiring the Next-Generation of Cyber Security Professionals in Government, YOUTUBE (May 17, 2010), https://www.youtube.com/watch?v=nwlkcC5KMvA.

Participating in competitions earns certification credits for professionals. "Certs" like the CISSP and others require the professional to pursue ongoing study in order to maintain their certified status. Today, credits can be issued manually, but standardizing their issuance should be considered. Businesses can also incorporate competitions into workforce development and standard operating procedures.

As Nasrin Rezai, global CISO of GE Capital explains, "Not only in cyber but in other parts of the company, there are a lot of competition-style ways of promoting new idea generation. Sometimes organizations do it [competitions] one-off, or it isn't a part of their development and workforce planning strategy. We see it as a component of our workforce development. Annually, one business takes the sponsorship; we jointly share cost, and we make it happen. The challenge becomes when you consider it a side job, interest or hobby of the group, instead of a critical component of learning and development."

StackSmash is one example of a professional cyber competition. GE's annual IT security hackathon provides a gateway to cybersecurity at GE. By engaging professionals from IT functions to explore the limits of innovation for real-world security issues, GE has seen tremendous value in imaginative thinking and new tools as well as the by-products of enabling collaboration and building cross-business relationships.

Another professional development competition is GhostRed. This homegrown capture-the-flag competition, has expanded organically within GE over the past five years. What started as a volunteer-driven effort to excite and connect students with hands-on cybersecurity experiences, has now become a formalized GE program designed to

recruit top talent into the company.

XI. TEACHERS VS. STUDENTS

The interviewees frequently noted that today's students are not aware of cybersecurity as a field of study or as a career path. Where the students are uninformed, so are the adults — the parents and educators. In fact, the gap between adults' skills and students' skill is growing: today's first grade children are proficient in the use of smart phones and tablets because these devices have been in existence and widely available since their birth. They know more than their teachers and parents about the use of tablets.

Educators, parents, coaches, and the wider education complex must be made aware of the subject of cybersecurity. Similarly, senior executives and boards of directors in the typical business are largely unaware of the threats their companies face, their need to defend them, and how to do so. Education and training is critical across the board for leaders – educators and corporate leaders – to increase the effectiveness of cyber education in schools and cybersecurity processes in businesses.

"I think cyber education is about teaching how things actually work. You need to understand how the Internet works and how packets work. For many people the computer is more of a black box than their car. They know their car needs gas, that it needs maintenance; there are inspections; they need a driver's license. They can drive around (in) this big, scary thing, because safeguards have already been established. But the computer, and the amount of damage that can be done to a person's reputation and identity — people don't get it. Cyber education needs to be about explaining how the Internet and networks work; this needs to begin as early as elementary school." – Laurin Buchanan,

CISSP, Principal Investigator Applied Visions, Inc., a division of Secure Decisions.

School systems have numerous priorities vying for attention and investment, and because they are charged with the care and nurturing of youth, they are generally risk-averse. Therefore, changing the education system is not easy to do. But if education is about teaching critical skills, Laurin Buchanan suggests "(We must) graduate useful, intelligent members of society and workforce; and we haven't done that with cyber."

Many interviewees made comparisons to their own high school curricula in their analogies to today's need for cybersecurity education: health class and hygiene, physical education, driver's education, home economics and trade/manufacturing-related courses were widely taught, because they were considered critical life skills. These interviewees asserted that the current prevalence of technology and related threats indicates that cybersecurity education can be viewed on equal footing with other subjects taught in schools. Training educators on cybersecurity issues can be made a higher priority; just as driver education instructors are expected to have a driver's license, all educators can be expected to have a general working knowledge of cybersecurity.

XII. STANDARDIZATION VS. THE SPEED OF CREATIVITY

The subject of standardization in the realm of cybersecurity and competitions was not greeted with much enthusiasm by interviewees. In an arena where speed, adaptability and creativity are core defining tenets, there is resistance to adopt standards that may encumber innovation.

There is great reluctance to overlay the process of proposing, developing, agreeing upon, and adopting standards. But when discussing creating, executing, and expanding competitions, several areas were identified where a standard approach would be beneficial to deliver economies of scale in an environment of scarcity.

Areas for standardization and collaboration across competitions include:

- Tools. Competitions involve labor intense processes for injecting actions into game play, tracking competitor progress, and scoring individual and team performance. Interviewees recommended automated solutions: Facebook's Capture the Flag platform, Leidos's Cyber NXUS, GE's GhostRed, the Air Force Association's CyberPatriot competition engine, and Secure Decisions' Comic-BEE, a "choose your own adventure story" platform).
- Scenarios. Competitions continuously require new scenarios to challenge the participants, especially returning participants. Collaborating on scenario development and developing standard taxonomy were identified to mitigate this challenge.[16]
- Resources. Effective and challenging events are resource-intensive. Cyber experts develop and run the game, and may participate as red teams. Scaling and expanding competitions must address staffing needs, to consolidate and centralize staff or knowledge.

[16] Bryan Fite, global account CISO for British Telecom, mentions a Scenario Development Language (SDL).

- Taxonomy. A dominant theme throughout the interviews was the need to standardize the taxonomy – the roles and definitions – in the cyber security workforce, both for competitions and in a professional environment. A human capital perspective was often repeated: establish better defined team roles that can be commonly understood across organizational and industry boundaries. There were also frequent analogies to sports, with their rulebooks and roles: a football team has a quarterback, defensive linemen, receivers, tackles, as well as a trained, focused and dedicated coaching staff.

"Everyone gets excited about competitions and wants one of their own; but it's a matter of scaling up with a 'force multiplier' and expanding the reach. There is a cost associated with the competitive platforms and engines. They take time, money, and people to develop and update them. If you've ever had to manage the logistics for one of these events, you know what it takes to do it." – Dan Waddell, Regional Managing Director, North America Region, (ISC)², Inc.

XIII. FUN AND GAMES VS. MEANS TO AN END

Among other objectives, cyber competitions, like other games, should be fun. While interviewees assign a high entertainment value to cyber competitions, a non-expert audience may likely disagree, which is one of the primary barriers when discussing cyber competitions as a competitive sport. The fun comes from meeting the

challenge, learning new skills, working on a team, socializing with competitors and sponsors, and achieving success.

To attract the workforce of tomorrow, or the younger generations, gamification, rules, teams, and scoring are believed to be highly effective. But a stronger argument for gamification of the cybersecurity arena might be that those competitive elements — process, teamwork, and results — are precisely what it takes to construct an effective cyber workforce.

One of the reasons that cyber competitions are seen as effective and fun is that they maintain a safe environment and eliminate the pressure that comes with the scoring and grading that happens in the classroom. Davina Pruitt-Mentle, lead for the NICE's Academic Engagement at NIST, says competitions "allow students to engage in an informal, non-threatening way, unlike in the classroom where they are graded. If we insist on scoring them, we will turn off some kids, because it takes them out of their comfort zone and away from the idea that they are just going out and having fun."

Because the games are fun, competitions can lead to other endeavors: attracting students to STEM fields, and stimulating creative thinking and innovation through intellectual problem-solving. Clearly STEM education is critical to national security, as the *21st Century Science, Technology and Innovation Initiative for America's National Security* report from May 2016 asserts;[17] cyber competitions are compelling method of attracting students to

[17] *A 21st Century Science, Technology, And Innovation Strategy for America's National Security*, WHITE HOUSE (May 2016), *available at* https://www.whitehouse.gov//sites/default/files/microsites/ostp/NSTC/national_security_s_and_t_strategy.pdf.

STEM.

However, competitions are not just about education and learning. Nasrin Rezai says, "We think that gaming/cyber competition is a key component of learning, education, and recruiting." Competitions, especially at the collegiate and professional levels, are ideally suited for individual competitors to demonstrate skills and for hiring managers in the government, defense sector and private industry to most effectively identify the best resources with the best skills. There were plentiful anecdotes in the interviews about jobs being offered to competitors at collegiate competitions. In 2009, Boeing, one of the sponsors of the Western Regional Collegiate Cyber Defense Competition (CCDC), hired the entire team from Cal Poly Pomona on the spot. In 2010, one competitor was pursued by multiple sponsors on the morning of the final day; they were too late; he was offered a job over breakfast. These examples suggest that competitions might be considered auditions for potential cybersecurity professionals.

These discussions explored whether the games themselves, and the outcomes – increased skills and cyber practitioners – could be expanded through standards. Competitions have been significant growth, with up to 40% increase in participants over the past few years.[18] Over the past few years, participants in competitions have increased by 40%. We asked: is a standardized approach unnecessary? Or does the lack of a trained workforce and the rapid advancement of technology justify intervention?

Professional certification is built upon standardization, and as such we explored whether competitions can benefit from an association with

[18] As cited by Bernie Skoch

professional certification. Dan Waddell from (ISC)^2 indicated that currently, a manual calculation process determines whether a candidate's participation and performance in a cyber competition can contribute to the professional development component of maintaining CISSP certification. Expanding competitions, particularly at the professional level, and advancing consistency in their processes and measurement, would facilitate organizations like (ISC)^2 accepting them as valuable skills development tools and as a part of the certification process. If it served their need to achieve and maintain certification, more professionals would participate in competitions to improve their skills.

Envisioning the potential reach, structure, and impact that cyber competitions might have, several stakeholders rely on the sports league analogies. Sports leagues, for example football leagues, have:

- Standard rule books (with age-appropriate adaptations as needed).
- Defined roles and responsibilities on a team.
- Organized events at multiple levels from Pop Warner to the NFL.
- Booster clubs and leagues.
- Sponsorships and television rights.
- Recognition for teams and individuals, like Heisman Trophies and Super Bowl rings.
- Large, passionate audiences and fans.

These attributes work in concert to elevate awareness of and passion for the sport, and attract athletes to the sport from a very early age. Apart from the love of the game, an athlete's prospect of making a career from the sport is limited. The numbers tell the story: There are approximately

1 million high school football players in the US[19] and under 2,000 players in the NFL.

The cybersecurity field provides a contrasting image. With 2 million jobs waiting to be filled, the prospects are great for young cyber athletes to find employment (after study, practice, and demonstrating his or her abilities) are on the playing field.

XIV. RECOMMENDATIONS

The opinions and narratives of interviewees reflect different approaches and varying priorities regarding:

- Cybersecurity skills development
- Offensive and defensive roles
- Awareness, education, and workforce development

The opportunity of competitions—to raise awareness, develop skills, and build a pipeline of cyber professionals — encourage a national dialogue of stakeholders from diverse constituencies:

- Founders and long-standing sponsors of the leading competitions in the US, such as CCDC, CyberPatriot, the US Cyber Challenge, Day-Con, the Atlantic Council Policy Challenge, DEFCON and others.
- Government agencies responsible for developing cyber skills, including the NSA, DHS, and the Department of Education.

---

[19] Terrence Jeffrey, *Football Is Top Sport in U.S.: 1,088,158 High School Players*, CNS NEWS (Feb. 2, 2014), http://www.cnsnews.com/news/article/terence-p-jeffrey/football-top-sport-us-1088158-high-school-players.

- Education systems at the federal, state and school district levels.
- Defense contractors who significantly invest in competitions, for skills development and recruiting.
- Private industry, which faces a skills shortage and is well-situated to develop and distribute tools to enable competitions and accelerate product development and differentiation using competitions as a proving ground.

The dialog should focus on building consensus in all areas involved with and impacted by cyber competitions and cybersecurity skills development. "If you impose structure — a taxonomy, an environment — it is much easier to roll out competitions across the USA and beyond," says Tony Cole, Vice President and Global Government CTO of FireEye, Inc. "But you also put on handcuffs; what is unique about the cybersecurity industry is that people think differently. This is how they find the unique vulnerabilities in systems. They don't go after things in a structured manner. A vast majority of cyber experts are self-taught. So, we need a structure that can be replicated; but we must ensure there is enough variance to allow 'out of the box' thinking."

The objectives of this larger dialog should:

First, agree upon areas where collaboration and standardization can facilitate expansion to a larger audience across geographies, age groups, school districts, and public and private enterprises without dampening the creativity and innovation paramount to keeping pace with the attackers.

Second, explore how shared investment in technology and process can both compensate for and

develop areas of competition that are otherwise limited by resources (people) and sponsors (funding).

Finally,, accelerate the advancement of the following aspects of competitions as well as the cybersecurity workforce as a whole:

- Standardizing performance measurement at the individual and team level across competitions. "It's great that everyone wants more cyber competitions, but without 'division rules' it makes it difficult to judge the relative value of one competition versus another. Without knowing whether the A team from one competition is as good as the A team from another, it isn't an effective hiring guide." Bobbie Stempfley, Director of Cyber Strategy Implementation, the MITRE Corporation.
- Aligning competitions with the NIST Framework. "The goals of the NIST NICE Working Group competitions subgroup are in sync with industry: to advance and identify skilled people ready to fill the growing needs of the workforce. The NICE Cybersecurity Workforce Framework is a great place to start to begin to understand the relationships between competitions that develop proficiencies in cybersecurity knowledge skills and abilities and employers who value those knowledge, skills and abilities tie to perform vital tasks in cybersecurity work roles." Bill Newhouse, Deputy Director, National Initiative for Cyber Security Education (NICE).
- Developing and sharing competitive platforms. "Until you've done one, you don't know how

critical and how difficult it is getting the competition environment working. You need a willing partner, usually a college or university, to host and deliver the resource intensive tasks of providing working computers, a functional wireless network, enough bandwidth from the ISP, and so on." Dan Manson, Professor and Department Chair in Computer Information Systems at Cal Poly Pomona/Co-Chair NICE Working Group Competitions subgroup.

- Developing offensive and defensive scenarios. "From my military background, I know that my ability to attack informed my ability to defend. You can't only teach defensive tactics that have limited application in the broader marketplace. But teaching attack methods alongside defensive techniques will enable your teams to better prevent bad things from happening." Pete Clay, Principal, Zeneth Tech Partners.
- Defining roles and responsibilities within a team of competitors or professionals. "Security is a very broad field ranging from policies, standards and compliance to software engineering and application security. We are now focused on defining and communicating the variety of security roles and how and where they fit into our corporate environment. There isn't a single path into security: there are different skills and techniques and tools to advance a career down a desired path." Jenn Henley, Director of Security, Facebook.

- Training the trainers to enhance educator skills. "It's important to understand what is age-appropriate, train the educators, and give them the tools to teach. A good analogy for teaching cybersecurity is teaching health; we teach children about hygiene, bacteria and germs first and then move on to more advanced topics in the higher grades. They need to understand the risk to their personal health and the risk to their cyber health." Dan Manson, CPP/Co-chair NICE Working Group Competitions subgroup.
- Raising awareness among students, educators, mentors, and parents on the career opportunities for cyber professionals. "Kids don't say 'I want to work in the medical profession when I grow up.' They say 'I want to be a doctor, a nurse, a sonogram technician, an EMT.' They pursue specific roles that they have seen and understand what is involved, that they know who is helped by that person or that role. In the cyber arena today, there is almost no visibility at this level." Laurin Buchanan, CISSP, Principal Investigator, Applied Visions, Inc., a division of Secure Decisions.
- Establishing leagues and divisions to support a competitive ladder for varying ages and skill levels. "In 1971, there were 700 women and 78,000 men playing high school soccer. Today, 450,000 men and 390,000 women play at that level. For cyber, we want to create a showcase that holds up these mental athletes in as much esteem as physical

athletes are held up. More jobs, careers and economic impact will come from this arena than from physical sports, and hav[ing] competitive cyber leagues will bring that level of attention, excitement, support and awareness that the field deserves." Dan Manson, Professor and Department Chair, California State Polytechnic University.

- Developing Cyber as a Sport. "Cyber is more than IT. It is our behaviors, actions, and uses — most for good ends, but some for bad. Cyber games train us to know what we're looking for, as well as how best to respond. They develop leadership, communication, and teamwork skills in a group of people that typically are more introverted. By developing cyber teams that compete in games like sports teams do, we can establish a code of ethics and a non-military approach centered on collaboration and strategy that will create the workforce we need for the future." Jessica Gulick, CEO, Katzcy Consulting.

Both a great need and a great opportunity exist for all stakeholders in the cyber competitions community to come together to better define the end-goal. Whatever the differences of opinions and priorities, there are significant synergies across all participants; and these synergies can deliver accelerated results through collaboration, coordination, and standardization, while acknowledging that creativity and agility must be given a wide berth.

XV. A NOTE ABOUT NIST NICE, ITS CYBERSECURITY WORKFORCE FRAMEWORK, AND THE NICE WORKING GROUP COMPETITIONS SUBGROUP

The National Institute for Standards and Technology (NIST) is a non-regulatory agency of the United States Department of Commerce. Its mandate is to promote innovation and industrial competitiveness by advancing measurement science, standards, and technology for the enhancement of economic security and quality of life. The National Initiative for Cyber Education (NICE), led by NIST, is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our Nation secure, and provide leadership.

NICE (http://csrc.nist.gov/nice/nicewg/index.html) brings together public and private sector participants to develop concepts, design strategies and pursue actions that advance cybersecurity education, training, and workforce development. Within the Working Group, subgroups focus on specific topics. The Competitions subgroup is responsible for conceiving this paper and encouraging all contributions.

The NICE Cybersecurity Workforce Framework (a.k.a. the NICE Framework and NIST Special Publication 800-181) provides a blueprint to categorize, organize and describe cybersecurity work into specialty areas and work

roles that include specific tasks and knowledge, skills, and abilities (KSAs). The CWF provides a common lexicon to discuss cybersecurity positions and roles. It provides a common language to speak about cybersecurity work roles and positions/jobs, and is a reference to help define professional requirements in cybersecurity.

The NICE Framework organizes cybersecurity work into seven high-level task categories:

- Securely Provision
- Analyze
- Operate and Maintain
- Oversee and Govern
- Collect and Operate
- Protect and Defend
- Investigate

As the stakeholder community called upon to explore the common themes and priorities for developing cybersecurity skills, the NICE Framework will provide a starting point to create taxonomy and encourage standardization that will accelerate growth and expansion.