Journal of Cybersecurity Education, Research and Practice

Volume 2023 | Number 1 Article 3

July 2023

Case Study: The Impact Of Emerging Technologies On Cybersecurity Education And Workforces

Austin Cusak
Robert Morris University, austin.cusak@gmail.com

Case Study: The Impact Of Emerging Technologies On Cybersecurity Education And Workforces

Abstract

A qualitative case study focused on understanding what steps are needed to prepare the cybersecurity workforces of 2026-2028 to work with and against emerging technologies such as Artificial Intelligence and Machine Learning. Conducted through a workshop held in two parts at a cybersecurity education conference, findings came both from a semi-structured interview with a panel of experts as well as small workgroups of professionals answering seven scenario-based questions. Data was thematically analyzed, with major findings emerging about the need to refocus cybersecurity STEM at the middle school level with problem-based learning, the disconnects between workforce operations and cybersecurity operators, the distrust of Non-Traditional Training Programs, and the need to build digital security generalists' curriculum and training. Recommendations are also made for possible next steps.

Keywords

Artificial Intelligence, Cybersecurity Career Pathways, Cybersecurity Education, Cybersecurity Workforce, Digital Divide, Emerging Technologies, Generalist, Higher-Ed, Machine Learning, Middle School, Multi-disciplined, Non-Traditional Training Programs, Problem-Based Learning, STEM, Workforce.

Case Study: The Impact Of Emerging Technologies On Cybersecurity Education And Workforces

Austin Cusak
Cybersecurity and Infrastructure Security Agency (CISA)
Robert Morris University
Alexandria, Virginia, USA
austin.cusak@gmail.com – https://orcid.org/0000-0003-2175-8753

***Abstract* – A qualitative case study focused on understanding what steps are needed to prepare the cybersecurity workforces of 2026-2028 to work with and against emerging technologies such as Artificial Intelligence and Machine Learning. Conducted through a workshop held in two parts at a cybersecurity education conference, findings came both from a semi-structured interview with a panel of experts as well as small workgroups of professionals answering seven scenario-based questions. Data was thematically analyzed, with major findings emerging about the need to refocus cybersecurity STEM at the middle school level with problem-based learning, the disconnects between workforce operations and cybersecurity operators, the distrust of Non-Traditional Training Programs, and the need to build digital security generalists' curriculum and training. Recommendations are also made for possible next steps.**

***Keywords* – Artificial intelligence, cybersecurity career pathways, cybersecurity education, cybersecurity workforce, digital divide, emerging technologies, generalist, higher-ed, machine learning, middle school, multi-disciplined, non-traditional training programs, problem-based learning, STEM, workforce.**

I. Introduction

Cybersecurity is going through the process of professionalization [13] with many policies, processes, and standards yet to be established [15]. One of the government entities working towards establishing norms and standards for the profession of cybersecurity is the National Initiative for Cybersecurity Education (NICE) within the U.S. Government's National Institute of Standards and Technology (NIST). Yet as advances in technology are made, so does the need to protect and defend that technology – thus while emerging technologies push innovation, often in risky ways, new technologies such as Artificial Intelligence (AI) and Machine Learning (ML) have yet to be integrated fully into cybersecurity [18]. Understanding and creating a workforce that can protect emerging technologies will likely be in high demand within the next five years and will be a critical element in the sustained protection of U.S. Critical Infrastructures [15].

The general and role-specific competencies needed for cybersecurity work are still being refined as the profession continues to evolve [21] with automation and other emerging technologies still needing integration into the current framework. Reference [2] argues that it will take time for cybersecurity professionals to understand the full scope of how emerging technologies such as AI and ML will be integrated into their work roles, hunted for when used by adversaries, mitigated when found in systems, and defended against. The NICE Framework developed by NIST acts as a unifying source for cybersecurity professionalization, pulling together experts from government, academia, and industry ("the private sector") to begin addressing issues like these [21], with one such method being NIST's National Initiative for Cybersecurity Education Conference and Expo.

A. Case Study Preparation

The 13th annual NICE Conference and Expo was held in Atlanta, Georgia, from 6-8 June 2022, addressing the theme *Demystifying Cybersecurity: Integrated Approaches to Developing Career Pathways* [16]. The goal of this year's annual conference was to bring together professionals from academia, industry, and government to work towards the NICE Strategic Plan's goal of "promoting discovery of cybersecurity careers and multiple pathways" [16, p.2]. This researcher became involved with the effort a year before the event in June of 2021 after being nominated by their federal agency to participate on the planning committee, which consisted of 15 volunteers from academia, industry, and government. Committee members were asked to give four-hour workshops to kick off the event [16].

In September of 2021, the researcher began working with a cybersecurity workforce expert from industry to co-lead the workshop, bringing new perspectives into creating an event that could be more meaningful by contributing to future iterations of the NICE Framework while pushing the professionalization of cybersecurity. Original discussions for the workshop were focused on gaining a deeper understanding of the obstacles to incorporating automation (specifically AI/ML) into more cybersecurity workforce training, as well as programs designed to train post high school learners (e.g., colleges, universities, trade schools, etc.,) referred to in this article as "higher-ed." and cybersecurity workforces. Identifying that the proper career pathway and skillsets needed for this newer multidisciplined type of work role were undefined; the researcher and workshop co-leader debated if a pathway for this type of complex role would be more effectively learned through a university/college program or a hands-on Non-Traditional Training Program (NTTP) focused specifically on technical skill development.

Additionally, as the researcher prepared for the workshop by asking questions to educators and field experts, another question arose as to whether or not higher-ed was enough time for students to gain anything more than a basic technical foundation, pondering if the real responsibility lay with employers who needed more robust internal technical training programs, with or including extended apprenticeships, instead of relying on students being ready for advance work upon graduation.

Following this was the debate on how to prepare high school students for potential cybersecurity careers that incorporated emerging technologies of AI and ML. The time a high school and even higher-ed student has to learn one discipline, let alone three, comes at a cost of technical depth that may or may not be what government and industry need in their 2026 workforce – and the need is apparently already here [24]. This raised the issue of trying to understand what employers should be requesting academia to put into their curriculums at all levels to prepare the cybersecurity workforce of 2026: Is it better for them to be completing their training programs with a wide diversified skillset that is narrow in depth, or is it more marketable to ensure students gain deep knowledge in a single functional subject? Both are likely necessary for training future workforces, but the broad or narrow skillset will likely need to be prioritized as the normal process, as discussed by [7] and [25].

The next issue debated was if the NICE Framework will be able to update fast enough to be the roadmap high school and higher-ed curriculum developers map to, or if industry and government employers will need to provide more frequent and timely advice to academia on what is needed to prepare students for their upcoming workforce needs. One question that kept emerging was if the next generation should be required to learn both cyber and automation with equal competency, and if so, who will set the standard for that new role that the entire profession will accept and emulate? Research on similar subjects found that currently used pedagogies are not dynamic enough to prepare students to be effective upon entrance into a technology security workforce [6, 15, 20, 22], leading to the questions this workshop sought to begin answering.

B. Reason for the Workshop

The problem this workshop set out to address was to understand some of the specific training, knowledge, and skills organizations will need their workers to have by 2026 in order to incorporate emerging technologies with current cybersecurity skillsets. Automation, specifically Artificial Intelligence (AI) and Machine Learning (ML) is becoming more and more relevant to cybersecurity [18] but is not currently being incorporated in cybersecurity education programs, workplace training, or U.S. STEM programs [24]. The workshop was set up therefore to answer the following two questions:

> RQ1: What types of training should be taught to high school, higher-ed, and current professionals in order to be capable of doing cybersecurity with and against AI/ML?
>
> RQ2: At what level of education does foundational training really need to begin, and should that learning be multidisciplined at the expense of being skill ready for a workforce, or should it be focused on a few key functional areas employers need upon graduation?

To find answers, a three-person panel of experts was brought in to share perspectives and insights, followed by attendees working in small groups to answer seven questions exploring different aspects of RQ1 and RQ2. The intent of the workshop thus became a qualitative case study where data could be collected from both a panel of experts and a room full of subject matter professionals whose ideas and recommendations could be thematically analyzed for the betterment of the cybersecurity profession. The significance of the workshop study was to help those in the federal, academic, and industry spaces begin determining what a new cybersecurity/automation work role could look like, who would need to lead different aspects of its creation, and what age students should begin learning about it.

Acknowledging that the topics this workshop addressed were not mainstream or widely defined functional areas within most cyber ecosystems, the questions to panelists were designed with the additional intention of creating awareness/exposure of AI/ML amongst the group of cybersecurity professionals attending. An acceptance by any cybersecurity leader attendees for a need to take action before a positional crisis arises was an additional intention. The workshop was thus structured in the hope that it could reach multiple goals: To collect data on RQ1 and RQ2, to shift perspectives of attendees on the need to train their organizations in these emerging technologies, and to help possible workforce leader attendees debate their counterparts from other sectors of the profession to begin deciding who should begin taking actions to further the process of professionalization.

With these goals in mind, the researcher established the following learning objectives for the attendees: 1) To openly explore upcoming challenges and potential opportunities cybersecurity organizations will have through more widespread implementation of artificial intelligence, machine learning, and the general incorporation of emerging technologies. 2) To attempt the identification of which competencies will be needed in our near-future work roles because of technological changes. 3) The allowance of debate amongst all present about the benefits and tradeoffs of educating generalists with a diversified skillset over training specialists with expertise in a focused area. 4) To openly discuss the need for determining which competencies or skills will allow current cybersecurity practitioners to quickly adapt to upcoming and current technological changes. 5) To identify which sectors of the profession (academia/industry/government) will need to lead specific programs, manage changes, and initiate efforts to ensure success over the next five years.

These objectives were viewed as specifically relevant considering [5] found that Digital Security organizations have dramatically shifted from being rigid to more loose networks to keep up with ever-changing challenges in securing information

systems. In this new way of working, having one technical expertise alone isn't enough for a professional to be truly effective in organizations requiring increasing multidisciplined skillsets in their subject matter knowledge. On top of technical expertise, the cyber security professional in this new type of environment needs to understand human behavior as well as organizational processes to meet the ever-changing challenges [5, p.121] since human factors often remain the weakest link in securing data and information [14]. The new reality says [5] that information has become more valuable than ever before and is now a major target of threat actors capable of using advanced technology. The next logical step is for these same threat actors to use AI and ML to improve their criminal activities which many are already adapting [4].

II. The Workshop Structure

The workshop was capped at 50 attendees, many of whom could be considered experts in the field of cybersecurity workforce operations, with three AI/ML/Cyber education expert panelists. The workshop was created and run by two facilitators plus an Albert Einstein Fellow who provided STEM Subject Matter Expertise (SME) in the room. The four-hour workshop was broken into two sections: a two-hour panel discussion with Q&A followed by two hours of small groups working through the seven questions on posterboard quad charts. To baseline a common lexicon of terms between a combined crowd of professionals from academia, industry, and government, definitions of cybersecurity and automation were shared. *Cybersecurity* was defined as a broad term for the use of various technologies and processes that protect digital systems, programs, data, networks, and all devices within these systems [9]. *Automation* was defined by [9] as referring to the technique of minimizing human input where possible, with *Artificial Intelligence* and *Machine Learning* being the two most relevant examples. Therefore, the term *Cybersecurity Automation* would be used to reference the use of artificial intelligence and machine learning in security systems to sense, study, and stop cybersecurity threats automatically. In addition, not knowing the background and technical acumen of attendees, the term cybersecurity was explained to be linked to IT and IT Security in its origins but should not be used synonymously with the term *cyber*, which was used to refer to the broader ecosystem of activities and support elements of a Digital Security mission space [11].

Working with the assumption that many or even most of the participants did not know each other, the room was configured so that no extra tables were available, and only seven to eight chairs were placed around each 10-person round table. Chairs were also spaced for social distancing in the back and sides of the room for those desiring social distancing, and they were notified at the beginning of the workshop that for the second half they would need to join a group at a table for discussions. To ensure the audience could interact with each other and the panelist, the room was intentionally configured to encourage a casual, comfortable environment. One of the workshop facilitators called in remote, as did one of the panelists who was in another country. A camera was set up in the room so the online panelists could see those in the room, and multiple microphones were used so panelists, hosts, and audience members could all hear and speak to each other without lag. When the four-hour workshop started, an agenda was shared and prizes were displayed and placed next to the refreshments to encourage participation in the first game, as well as a trivia game that kicked off the second half.

A. Panel Discussion With Experts

The first half of the workshop consisted of a panel with experts from three areas: AI education, AI/ML operations in the security industry, and government cybersecurity higher-ed work. The last expert also works as a university adjunct teaching technical cybersecurity courses. The workshop facilitators also lent their expertise through the semi-structured interviewing process, sharing and debating their lived experiences and personal research about how cybersecurity and emerging technologies currently do/do not intersect. One focus of discussion was on which functional areas should be considered in possible future designs of a cybersecurity automation career pathway and what is currently in the way of creating one. To encourage comfort in challenging and debating ideas between panelists as well as the attendees, an icebreaker of two truths and a lie was used where each of the three panelists read a cutting-edge technology story, one of which was fabricated. The two people that guessed correctly were allowed to select prizes, visibly increasing the comfort and enjoyment of the audience.

To further keep audience members engaged, the AI security expert showed visualized findings from his own research, and the facilitators showed and discussed AI-generated images from *DALL-E 2*. Image examples [3] were shown of the author using the text prompt "A bowl of soup that is a portal to another dimension" that fabricated four pictures of soup ranging from a cave painting to a vortex of spinning colors in photo-realistic clarity. Also shown [3] were images from the website *Not a Real Person*, where a completely fabricated human and background were generated to a level of detail similar to a high-resolution camera. These attention tactics were used at strategic times to refresh the minds of both panelists and the audience, keeping the discussions moving and adding clarity to AI/ML conceptual discussion points. Findings from the panel discussion are in a subsequent section of this article.

B. Small Group Work In The Second Half

The body of participants from academia, industry, and the government had purchased tickets and arrived a day before the main conference, with the majority of participants consisting mostly of senior-level professionals from academia. There were also senior leaders and workforce representatives from industry, and only a few senior workforce development participants from the government. The RSA 2022 conference had been moved from April to the same week as the NICE Conference in June, which was believed to be the main driver for less industry and government participation in the workshops as in previous years. The conference and workshops were still well attended, and participation in each workshop was capped

to ensure quality discussions, but the mix of this year's participants lacked cybersecurity operations professionals.

Questions with places for input via writing and/or sticky note were provided in quad chart form to each table on large pieces of poster board. The groups were given instructions, and each table was allowed time to discuss and capture their ideas into four sections: *Ideal End-State*, *Key Activities*, *Challenges/Risks*, and *Next Steps*. Each table chose a spokesperson, briefed their findings to the room, and took a maximum of two questions from fellow attendees due to time constraints. Once briefed, that table's quad chart was hung on the back wall of the room, accompanied by a second clean quad chart for additional comments by other tables at the end of the workshop walk-about.

Anticipating the strong personalities and opinions of conceptually based senior leaders from different sectors conflicting with those of more tactical-level technical experts, a trivia game was used before quad charts were given to the tables to help cut through the potential awkwardness of being required to discuss and challenge strangers with unknown backgrounds. Since time was limited, this was deemed an effective way to remove any possible posturing since competition with rewards has been shown as an effective way to get strangers to bond through common experience by building consensus quickly to achieve a common goal [1].

C. Panel/Workgroup Engagement Methodology

For the first session, a semi-structured interview technique was used to probe panelists who had been provided the base questions and order beforehand. All panelists were encouraged to answer each question, with the hosts designating ahead of time which panelist each base question would be directed to first for better flow. The semi-structured interview process was chosen because it allowed for leeway in probing respondents' questions and gave the host/researcher greater dexterity in managing the flow of the interview/discussion [8]. One of the goals of having a panel instead of only conducting audience workgroups was to add context to topics the participants may not be overly familiar with. To do this, the flow of the base questions was carefully designed to start with a macro discussion of where the experts believed AI/ML/Cybersecurity will need to be in five years, then explore upcoming challenges for intertwining those emerging technologies into current and future cybersecurity work roles. The panel discussion ended in a micro discussion of specific skillsets needed to become a multi-disciplined security technology professional, including what competencies they observed academia needs to focus on growing in K-12 and higher-ed to create a cybersecurity automation career path.

Since interviewing was not used in the second part of the workshop, participants in their small groups were encouraged to give detailed answers specifically for the level of student or professional their group's problem impacted the most. The levels shared with attendees to consider were four groupings, the first being *pre-professional and/or K-12*: Those entering or in high school specifically. They were asked to consider the competencies and skills this generation may need as they become the workforce of the future, specifically circa 2026-2028. The second grouping to consider was *pre-professional and/or higher-ed*: Those post-high school who plan to enter the workforce through self-study, Non-Traditional Training Programs, apprenticeship, internship, college, or university. They were asked to consider what knowledge and skills these people would need to perform required tasks competently upon arriving at a work center. These were called the new workforce of 2023-2026. The third grouping was *early-professionals:* those already in a work role who are trying to determine a career path. They were asked to consider the competencies, skills, training, and experiences these early professionals may need to determine a fulfilling career path, as well as determine if their current skillset will be as relevant in 2026 as it has been in 2022. The final grouping was called *mid-career:* those who have already been doing cybersecurity for 5-10 years and have relevant competencies, skills, and experiences to grapple with new types of problems presented by emerging technologies.

It was the intention that these added scopes would help each group work through their problem with more clarity, creating data points that could be relevant and useful to cybersecurity's professionalization.

III. Questions And Findings

The two-hour panel discussion conducted in the method of a semi-structured interview received positive feedback from audience members in post-workshop and in-person polls. While all comments are worthy of further discussion, only a few topics of particular relevance to the RQs were explored in this thematic analysis for brevity.

A. Panel Discussion Findings

1) Panel Theme 1: The Best Time To Build A Foundation Is Middle School. Students in middle school are able to mentally shift from pure instruction to more lab work at this stage of educational development, making it easier to grab their interest with automation and technology security. It was previously believed that high school was the best starting point, but one of the panelists has found through both their academic and professional work in multiple countries that middle school students are particularly equipped for learning computer languages and doing hands-on experiences, such as sandboxes, labs, gamified challenges, and very narrowly constructed competitions. Working outside the U.S. they see the start of this interest begin in 4th grade, with a willingness to try, fail, and try again as many times as it takes to get desired results really emerge in middle school (7th and 8th grade specifically). Other countries with a more unified curriculum approach than the U.S. system are already doing this well, and in some regards, the U.S. is behind. To be on par with peer nations, it is the responsibility of state and federal governments to be nonpartisan in this regard, and the responsibility of industry to provide programs and training for this specific demographic to use freely without strings attached. Middle school is the best place to help students begin understanding how the different

emerging technology disciplines interweave and the right place to start practicing skills to build technical confidence.

2) Panel Theme 2: U.S. K-12 STEM Is Being Held Back By The Digital Divide. While some may see putting resources into bridging the Digital Divide as partisan and for states to determine, the consequences of students with the right technical acumen not being given the opportunity to learn STEM damages the U.S.' ability to protect its infrastructure and economy. *Prohibiting students from feeling personal justice and dignity, as well as a sense of belonging to the larger society* is more than just a moral imperative because of this. Emerging technologies don't currently fit within most STEM programs, which acts to widen the gap of the Digital Divide. The Digital Divide was defined for the attendees as the ever-widening gap in student/teacher/classroom/instructor populations, both culturally and digitally, between those with opportunities and those without [12]. This Digital Divide, therefore, does not only refer to schools having the equipment and access to current technologies but also the opportunities to learn and be trained in up-to-date methods and use of that technology so a student can be adequately prepared for a tech-based job [19]. One of the workshop attendees, an educator in the Chicago area, shared with the group their experiences of seeing school districts just miles apart where students in low-income families had very little to no opportunities to learn STEM, while those in a very near more affluent school had many opportunities, including sponsored STEM camps during the summer.

3) Panel Theme 3: K-12 Instructors Lack The Training, Equipment, And Support To Introduce Students To Cybersecurity, AI, And ML. The panel agreed that cybersecurity, AI, and ML are interrelated and are based on the same foundational concepts and skills, but they are not taught that way. A student could choose a path in one of the three or in multiple if they learn the foundation, but when teachers present AI/ML concepts in STEM, they don't cross over into security. The use of AI/ML to help security is a level of knowledge they are not trained to convey and are, therefore, likely to not engage. Additionally, AI/ML has become synonymous with *tech innovation*, which is often seen as hampered by security instead of a necessary aspect of the overall design. Curriculum must be built into STEM that allows students to explore the differences between these types of technologies, allowing the "T" in STEM to include both automation and cybersecurity. The Panelists agreed that the use of AI and ML will both become major areas of work within cybersecurity in the next six years, so resources must be provided to K-12 educators soon to get in front of the coming necessity.

4) Panel Theme 4: More Effort Outside Of K-12 Is Needed To Help Prepare Students For Careers. Following the lead of other developed countries, exposure to careers in emerging tech needs to happen while students are in middle school by non-academic entities, even though there is no profit for them in the short term. Computers alone used to be considered *high-tech* just by processing data and generating images, which is where many U.S. curriculums got stuck. Once everyone started using Smart Phone level technology, the enthusiasm for expanding the basics of STEM's "T" from computer science into an exploration of emerging technologies vanished. Too many became overly comfortable using technology they don't understand in their daily lives, allowing those in "Big Tech" to manage it for them. Hence, the excitement when a piece of new tech is released from excitement to expectation. But the challenge remains that tech and Digital Security need to find people with the right wiring and skills to successfully grow what is here, and traditional schooling and higher-ed aren't enough. Therefore, those outside of K-12 need to be connected with Non-Traditional Training Programs (NTTPs), tech schools, and tech apprenticeship programs. The survival of cybersecurity will rely on these programs, which also need to extend to AI/ML skill development and cross-training. This discussion line led the panel to discuss how the positive aspects of cybersecurity specifically can be a great profession for those with neurodiversity since a neurodivergent mind that is interested in a subject often comes with a deep well of curiosity and mental resiliency to keep trying new approaches with lateral thinking (in the room it was referred to as "thinking outside the box") until they solved the problem. For example, it was shared that personal experience has shown that those with ADHD and autism seem drawn to the profession of cybersecurity through non-traditional learning pathways and often find that the benefits of their particular neurodiversity help them more quickly identify problems and use different tools to get past challenges. Specifically for ADHD, the ability to hyper-focus on subjects the student finds interesting allows those with basic cybersecurity tools to mitigate constantly evolving issues. Similarly, those on the autism spectrum have been observed as being able to apply hyper-logical processing to deal with complex issues quickly and effectively, even in high-stress environments. No references were cited for these observations.

B. Workgroup Questions And Findings

At the end of the panel discussion, each of the seven workgroups were handed a question to answer, then time to brief their responses to the larger audience. Answers were captured on poster boards in four sections: *Ideal End-State, Key Activities, Challenges,* and *Next Steps.* Poster boards were hung on the back wall for a final walkabout once completed, and additional thoughts were captured separately for quality control on a separate poster board, then incorporated into the findings once they were vetted as relevant to the problem. The seven workgroup questions are as follows:

- Consider a generic high school STEM curriculum. What must be added to those curriculums in terms of activities and hands-on opportunities (labs, etc.) to give the students tangible experience?
- "What should we be doing to provide opportunities for our current middle school students to start down a path of becoming a professional in AI or ML or Cybersecurity OR

a mix of these, AND does industry, academia, and government have different responsibilities to make this happen?

- A high school junior comes up to you and says they are interested in possibly pursuing a career in "something cool, like AI or cybersecurity." They ask for advice on how they should approach learning these emerging technologies. They do not want to attend a four-year higher-ed institute. Should they try to find the one thing they might like and really hyper-focus on it, or should they try to become more of a generalist in multiple emerging technologies at the expense of gaining deep knowledge in just one subject? How should they approach gaining this experience?
- A high school junior comes up to you and says they are interested in possibly pursuing a career in "something cool, like AI or cybersecurity." They ask for advice on how they should approach learning these emerging technologies. They will be attending a university. Should they try to find the one thing they might like and really hyper-focus on it, or should they try to become more of a generalist in multiple emerging technologies at the expense of gaining deep knowledge in just one subject?
- Should we be teaching college students and Non-Traditional Training Programs to have a diversified skillset of using/working with emerging technologies, OR should we create programs that help them understand what they are very interested in and hyper-focus on gaining deep knowledge in one thing. Ideally both, but which is the priority and why?
- If we were to design a new category for the NICE Framework that combines Cybersecurity with AI and ML, what skills and knowledge would be needed as foundational for this position, and who would pilot and evaluate this new work role effectively to see if it's meeting the profession's need? (Meaning should it be tested first in industry, government, academia, or something else)
- Will those seeing more traditional type degrees (such as business, history, education, etc.) need to start gaining technical skills in AI/ML/Cyber? What are the most pressing cross-over skills these non-technical programs need, and who should have a role in developing these future programs?

C. Workgroup Themes By Section

While some unique findings surfaced from each question, themes emerged within each section that appeared in many if not all of the workgroup answers. These themes were captured within the four sections of *Ideal End-State*, *Key Activities*, *Challenges*, and *Next Steps.*

1) Ideal End-State.

a) End-state theme 1: layers of standards are needed. Creating standards for cybersecurity at all levels of K-12 that will lead to clearly defined employment paths was seen as very important. Having counseling and mentoring should be part of this, and aggressively screening for only hiring staff truly committed to the attitude of being "in this together" was held as a priority. Classroom teachers bare more responsibility. This responsibility was seen as needing to be extended up through higher-ed, so that when new professionals arrive at a work center, they already have a basic understanding of securing AI programs. Universities were seen as the actor needing to lead in the creation of degree programs that meet the specific need of the industry, which can then be used to update the standards K-12 should follow.

b) End-state theme 2: certifications should be pushed. Stackable certification was a common theme in conjunction with the need for a bachelor's degree. Despite the messages of the panelists, many workgroups did not have confidence that new professionals entering a cybersecurity and/or emerging tech profession outside of traditional routes would be prepared sufficiently. The ideal was seen as students in 11th grade beginning to earn certifications, then those same students being required to mentor younger students on their path as part of the continuing certification process. NTTPs were seen as a less effective option, but a distinction was made in that new and entry-level professions should prioritize gaining full certifications, with a concept of "micro-certs" being a way for them to show new skills in different emerging tech. For those already at the young and mid-profession level, certifications in NICE categories with micro-certifications geared towards multi-discipline cross-functions are needed.

c) End-state theme 3: shift the focus to middle school. The theme of addressing the Digital Divide was given a lot of attention, with multiple groups wanting a national focus from the government requiring all students to learn emerging technologies instead of it being just a STEM subject. Middle school curriculums were seen as needing to be the first area of government focus, providing a foundational level of technology with more opportunities for all students to pursue more advanced tech subjects. Industry and higher-ed were seen as playing a large role in creating authentic learning experiences for students based on real cyber work after government leads the way. Labs were also seen as needing financial and instruction assistance for building and maintaining the hardware and software instead of the complications and costs being on the school to manage alone.

2) Key Activities.

a) Activity theme 1: existing curriculum must be modified. Participants felt AI/ML and cybersecurity needs to be mixed, and the broader discipline of "cyber" needs to be incorporated into all school's information literacy courses. Baseline curriculums need to be adopted first, followed by customized sub-curriculum for functional areas that focus on hands-on training. Additional prep courses in STEM are needed in mixed cyber/AI/ML that include labs. Higher-ed and government both were seen as the entity responsible for creating this process.

b) Activity theme 2: collaborate the transition into higher-ed. High school students were seen as needing the most career help, with a proposal to give them access to assessments

and career coaching to gain direction, then be encouraged to enter a formal education program. ACT/SAT prep was also seen as needing to include a section on emerging technologies. High school students in the Digital Divide should be assigned a mentor and be encouraged to join university clubs, peer-supported meetups, externships, internships, and apprenticeships. The NICE Framework was mentioned as an important part of high school cybersecurity since all schools should map to it, not just higher-ed. All universities/colleges were seen as responsible for creating these shifts and should also be requiring an emerging technology overview course for all incoming science-related and undeclared majors to try and get more cybersecurity majors. Industry was seen as needing to work with higher-ed to provide support.

c) Activity theme 3: non-traditional training programs (NTTPs) are trending. There is not as much confidence in NTTPs as there was for traditional education pathways amongst the workgroups, but there was a recognition that "boot camps" specifically can be very useful in teaching students diverse skill sets. This was seen as an effort industry should lead.

d) Activity theme 4: make middle school the focus. Middle school education programs were seen as needing to be more multi-faceted, incorporating technical hands-on opportunities that allow for abstract problem-solving through multiple mediums of content. Ensuring people of different learning styles have more chances to engage with the content is seen as a responsibility of academia and government.

3) Challenges.

a) Challenge theme 1: the system isn't working. National and state standards were not seen as currently doing what's needed, with STEM being baked into general curriculums that require negotiation with teachers' unions to change. Industry, higher-ed, and government need to depoliticalize STEM curriculum, with industry playing a larger role in articulating the upcoming market needs. Participants shared that the market will always change faster than academia can make updates, creating higher-ed curriculum that is outdated on arrival. Higher-ed was seen as not keeping pace with the employment landscape needs, which was likely due to a lack of connection between industry and educational institutions in curriculum development. The need for clear pathways from high school should be established by both academia and industry, with industry needing to take the lead by conducting non-profit-seeking pathways that benefit society.

b) Challenge theme 2: the training is too intense. The need to get middle school students onto a multidisciplinary path is already hard enough, and getting students committed to lifelong learning is already a challenge. Participants shared that the basics of creating a solid foundation in math isn't happening yet, and there is apparently an increase in students leaving higher-ed programs due to a lack of motivation and an unwillingness to go into massive student loan debt. The participants also saw a lack of family/community support as a major obstacle to students finishing challenging programs.

c) Challenge theme 3: not enough access to resources. The Digital Divide was seen as a major challenge because it prevents students with the technical acumen from an opportunity to try. Funding is, therefore, the gateway to student success. Bootcamps, certifications, and equipment were seen as a costly but necessary way forward, with industry and government needing to do the heavy lifting by providing students significant discounts and creating more apprenticeship programs for high school level students. Tuition reimbursement for employees and loan forgiveness was seen as not enough to retain talent. There was also a concern that the lack of resources would force students to become more tech security generalists, only gaining a shallow knowledge of critical functional areas.

d) Challenge theme 4: traditional education doesn't work for all. Some of the workgroups believed that ADHD and other types of neurodiversity are often not discovered until after middle school, especially in underserved communities. While some of those neurodivergent minds could be excellent at cybersecurity and emerging technologies, they don't get the chance because they may struggle with traditional styles of schooling. Participants believed that a student who left high school without plans for higher-ed would likely lack career options, mentors, and money to pay for certification training and equipment. Those graduating in the Digital Divide have it worst. One workgroup observed that those who leave high school without higher-ed plans have difficulty with social interactions, lacking the ability to balance personal interests with the needs of prospective employers.

e) Challenge theme 5: no current nice category for AI/ML/cybersecurity. All workgroups agreed that a new NICE Framework category needs to be created that captures the Tasks, Knowledge, and Skills [17] needed to do *cybersecurity automation.* What this role needs to do, what the work would look like, how the training should be approached, etc., is to be determined. The ethical implications of emerging technology would also need to be clearly defined. Fear of Sci-Fi style AI issues crept into answers here.

4) Next Steps.

a) Next step theme 1: future programs must be developed together. All workgroups believed the process for addressing challenges and reaching ideal states is for professors, industry leaders, and government training leaders to collaborate in the development of a nationally based future program that could also be adopted by the international community. The place this centralized coordination of ideas could best happen is through NICE (part of NIST), which is already leading qualitative processes and working towards cybersecurity's professionalization. Designing higher-ed degree programs that incorporate the security of emerging technologies was seen as the priority in this effort, with no mention of NTTPs. A single taxonomy was also recommended for adoption between cybersecurity and AI/ML, ideally becoming a global standard. Ethics was seen as an essential root of all higher-ed training, and traditional models of teaching cybersecurity were seen as needing to be more hands-on.

b) Next step theme 2: foundational tech courses before middle school. Gen Cyber Camp and similar fun training for high school students were presented as needing to be simplified for younger audiences. The NICE Framework [17] was also seen as a possible standard for students, at least down to middle school, if not earlier. Creating benchmarked graduation requirements for high schoolers to win apprenticeships was seen as a possible avenue, with a push to change the national focus to students developing skills with emerging technologies. One workgroup proposed having NICE collect quantitative metrics measuring the progress of the middle school refocus effort so adjustments could be made. A different workgroup believed the best first step would be to have experts from industry brought in to work directly with middle school students instead of leaving complex disciplines for self-discovery only.

c) Next step theme 3: school districts need to request help and resources. The conflicts between state and federal standards were seen as a major battlegroup that hurt learners for partisan gains. Everyone believed having critical infrastructures secured was a non-partisan issue though, so curriculum "that works" needs to be developed and shared openly. Both government and industry should sponsor more training for K-12 STEM educators, with industry creating work-based learning opportunities for students to gain exposure to real-world issues. Big Tech companies like Apple, IBM, and Google can also be asked to provide massively discounted software and refurbished hardware for students.

d) Next step theme 4: non-traditional training programs should be expanded. Money talks. The workgroups believed government should fund employment coaching and formal mentoring for all students going through an NTTP, while coordinating internships and apprenticeships for both government and industry. Industry had the additional role of creating more entry-level positions instead of asking for unrealistic work experience in entry-level jobs. Multiple workgroups also said that agreeing on a standard technical position description language is a must. The pathway of a student leaving an NTTP with a prearranged apprenticeship was seen as necessary since these students were disadvantaged by not attending a traditional formal higher-ed program.

e) Next step theme 5: cross-disciplinary skills through NTTPs must be incentivized. Workgroups believed schools would need to work with local industry and/or government to build community Security Operations Centers (SOC) for skill practice and have career ambassadors to market NTTP programs. Providing childcare for NTTP students was seen as necessary, but not for traditional higher-ed. Earning money was seen as the goal of students entering an NTTP, so industry/government-building paid apprenticeship programs for recent high school graduates were the way forward.

f) Next step theme 6: a desire to make academia profitable. Two workgroups felt that many of the issues could be most easily addressed if higher-ed was allowed to focus on being profitable instead of non-profit. When questioned on this, they believed higher-ed is capable of effectively self-regulating with their current administrative mechanisms, allowing colleges and universities to better meet the challenges and requirements raised in the workshop.

IV. Analysis of Findings

A major unexpected aspect of the workshop themes was the high-level conceptual answers given by the attendees for all four areas. In designing the workshop, an assumption was made by the researcher that most of the participants would be current and former cybersecurity professionals who had conducted actual operations, analysis, or done work in a cybersecurity functional area. The workshop and questions were therefore designed to produce more tactical level answers from those with direct knowledge of Tactics, Techniques, and Procedures (TTPs) that could be adopted for K-higher-ed audiences. Instead, the majority of participants were from academia and/or workforce operations, which likely did not generate themes the same as a workgroup with a fuller mix of former technical and current workforce professionals working together would have. However, two of the panelists stayed and participated in different workgroups, producing more actionable next steps and fewer conceptual-level answers, which may have impacted the overall findings.

A. First Major Findings: There Is A Disconnect Between Those Conducting Cybersecurity Operations And Those Supporting Cybersecurity Workforces

Some workforce operations professionals don't understand their cybersecurity workforce if they have never done actual cybersecurity work. Cybersecurity has too many entrance pathways and seems resistant to what has worked for IT and IT Security workforces, which is pushed upon them by workforce operations professionals. Traditional workforce best practices do not seem to be working, and those making decisions about future workforce needs are doing so without the technical experts giving them the right information to make workforce decisions. There is also a disconnect and even disbelief that cybersecurity needs to be approached differently by longtime workforce operations professionals. The move from OPM's KSA to the NICE TKS is a compelling enough reason to update best practices. Therefore, the NICE Conference needs to become a place where workforce operations, technical trainers, and current/former cyber operations meet and work together to determine needs, next steps, best practices, and points for collaboration. Workforce operations showed up in force at the conference, but very few cyber operations and training professionals were present. Workforce operation leaders must embrace new ways of working with this currently untraditional workforce and prioritize new pathways that allow employees into their organizations, such as NTTPs. Many with the right technical acumen are not entering the profession because the pathways are too traditionally based. This is also just for cybersecurity, not including emerging technologies. One point of note, understanding potential competencies for a career pathway in c*ybersecurity automation* was mentioned multiple times, but only one workgroup (with an AI panelist) provided context on the subject. All other answers, solutions, and ideas

were kept at a very conceptual level, leading to learning objectives two and four being mostly passed over. The NICE Framework's more refined TKS was not discussed, which was a missed expectation of the workgroups who were attending a conference hosted by NIST's NICE about the Framework. Discussing the NICE Framework's move away from OPM's limited KSA model into the TKS model was never fully explored, even though the TKS model better reflects the cybersecurity professionals' work roles. KSA's were mentioned frequently though. There were also a lot of incorporated ideas from the panelist in workgroup answers, but respondents seemed unsure of how to use the AI/ML information, which was more hinted at than anything else.

B. Second Major Findings: New Methods Must Be Adopted Across All Education Levels

Using Problem Based Learning (PBL) tactics, cybersecurity must be woven together with emerging technologies such as AI and ML, which are already being used by Advanced Persistent Threat Actors (APTs) against ALL sectors of the U.S. [4]. AI is already being used against schools, hospitals, and businesses, requiring organizations conducting security to invest in building professionals that can respond with the same technologies. Younger professionals need emerging training opportunities, which businesses seem reluctant to do. The cybersecurity industry is still relatively new and considered transient, which employers may see as a sink of their time and resource. Providing expensive training just to have people walk to a different job with their new skills is a necessary risk. More entrance points from NTTPs and apprenticeships should therefore be prioritized, with Continuing Service Agreements and incentives tied to demonstrated skill execution post training to receive higher compensation. Recognizing the importance of finding new ways to attract and retain talent, the U.S. Department of Homeland Security (DHS) for example has created a Cyber Talent Management System as a means to bring in and keep good talent by providing higher compensation for demonstrated skills and performance. Overall, the system was seen as not working, and those from academia shared the need to make academia more profitable so it could solve the many challenges of the workforce. When asked in the event how academia, in general, would effectively self-regulate and not become even more cost-prohibitive than it currently is, the answer was government subsidies without oversight. This response could have been from a variety of experiences, but it was unfortunately not explored further in group debate due to time constraints.

C. Third Major Findings: Middle School Needs To Be The Focus Of Resources First

The curriculums of good STEM programs should be ported into middle school-level labs, with intentional sharing of best practices and open-source materials. National and state education leaders must press the importance of getting more emerging technology into middle school classes, with emphasis on the need to address the Digital Divide. Addressing the divide is not only the morally correct course of action but also an action that will benefit the larger society by finding individuals with the right technical acumen that can do security of emerging technology well. The starting point for all middle schoolers, including underserved communities, is to consider making current materials more engaging and hands-on using PBL.

D. Fourth Major Findings: Build Security Generalists First Instead Of Functional Area Experts

Findings from the workgroups were that a majority of participants at the workshop felt focusing on creating broad technical security generalists was less effective than more focused degree programs specifically geared towards a few different cybersecurity functional areas. The panelists believed the opposite, saying that all STEM students should be taught as technology generalists regardless of their field since all STEM has multiple crossing points now and will have even more by 2026. The need to focus on just one functional area was still seen as more important, with faith in certifications ability to verify expertise in the skills. However, it is unknown what tactics APTs will use against U.S. societal interests in 2026-2028, and an overreliance on certifications as skill verification is not likely the way forward. When things are moving fast, having more broad skill ranges is more ideal since it will be easier to dive down into any one functional area if a baseline has already been established. One panelist also shared their experience that AI/ML and emerging technology specifically is a more complicated functional area to learn than cybersecurity and that AI/ML should be prioritized with students since it's easier to move from AI/ML into cybersecurity work than learning AI/ML after having only a cybersecurity skillset.

E. Fifth Major Findings: Current Workforce Operations Does Not Trust NTTPs

One unexpected observation from this specific point was how current young professionals are viewed by the majority of senior-level participants in the workshop. Traditional higher-ed is still seen as the only real option for a career. Participants of the workshop were not fully swayed by the combined panelists' insistence that traditional education isn't enough. The workgroup results showed a mistrust of NTTPs, believing colleges and universities were the only trustworthy path to a good career. Four workgroups showed a clear distrust of NTTP students' success trajectory while holding high trust for completing a traditional higher-ed program. NTTP students were believed to need more financial help from their families, a high need for childcare, and support networks that could mentally help them get through training. The researcher also captured participants' perceived challenge that those who did not attend a university/college would have difficulty with social interactions and have a harder time becoming functional adults. It is possible these workgroups did not have experience with students coming from NTTPs and were unaware of the successes NTTPs have had in placing their students into apprenticeships and entrance-level work roles. While NTTPs may not have the same length of time as a traditional higher-ed institution, they are often based in PBL and push skill development through interacting with real-world problems, making them ideal apprentices in fast-paced cybersecurity operations centers. While apprenticeships still need to be

standardized with a focus on teaching new hires their responsibilities, NTTP programs are one effective way to address the Digital Divide and underserved communities specifically.

V. Additional Recommendations

A large amount of qualitative data addressing parts of RQ1 and RQ2 was analyzed and shared thematically above. Themes would possibly have been different and more detailed if the workshop had been more balanced with technical perspectives, which would have required more operational-level professionals and experts from cybersecurity and AI/ML to be present. Workforce operations and academia representatives showed up, but their government and industry trainers and educators did not.

One major finding from this event was the agreement that foundational training needs to start earlier than it currently is and that such training must incorporate emerging technologies and Digital Security. Since this is a large concept that is easy to say but challenging to put in motion, a goal using data from the workshop was formed for educators to consider: Begin building foundational content that *evokes curiosity*, which is a crucial component for students to *practice adaptability*, leading to them gaining a baseline of *technical confidence*. Any activity fostering this process should be a good start since the panel of experts believed that technical confidence can be grown into high technical acumen. Therefore, to supplement what was shared in the findings and analysis section, additional recommendations gathered from the panelist, the workgroups, and pre-work group preparation are presented below for consideration of some steps that might help initiate more development opportunities for cybersecurity and AI/ML cross-disciplinary approaches.

A. Professionalization

The Office of the National Cyber Director (ONCD) should have more operational-level counsels supporting the growth of the NICE Framework by bringing together industry, academia, and government. Professionalization is the goal, and the government has a unique role, with ONCD taking lead in creating policy, NICE in framework and competency mapping, and CISA in sponsoring NTTPs, competitions, cyber ranges, and more 7-12 grade engagement programs. Industry, especially Big Tech, could take a larger role in providing equipment, free training, and apprenticeships while also providing annually updated work role requirements to academia. Academia can update their curriculum to prepare students better and create NTTP satellite training for their geographic communities, possibly subsidized with government grants. The ONCD should also begin the licensing process for key cybersecurity roles, including determining which certifications are most applicable to work roles and standardizing those.

B. Make Training Fun For Middle Schoolers

Students need to be given hands-on opportunities to dabble with tech, software development, and being administrators of systems instead of just users. The ideal is to get students to understand the basics of cryptography in security systems before high school, which would likely be more effective with some form of mentorship from outside of the school. If this process is successful, it could be considered a standard for schools within the Digital Divide. To start this off, industry and government could allow cyber ambassadors to speak with students, share cyber stories in classrooms, and build connections with teachers who are starting out in this area of STEM. Gen Cyber Camps and Cyber Patriot are current programs that could be expanded downward from high school to middle school for this purpose, with industry taking the lead to create roadmaps for apprenticeships and free training that grows with the grade of the student. Middle school students should be encouraged to gain more than a basic knowledge of computer languages and be given hands-on learning experiences such as sandboxes, labs, gamified challenges, and very narrowly constructed competitions. The goal needs to be to allow them to try, fail, then try and fail as many times as it takes to build their adaptability muscles. They also need to learn that it's okay to fail... that's how they learn.

C. Shift To Broader Foundations That Incorporate Emerging Technology

While the workgroup participants felt that a shift to find classroom teachers more committed to learning and teaching STEM was needed without additional compensation articulated, the classroom teacher does have a vital role and therefore needs prioritized support. To prepare 7-12th graders for NTTPs and higher-ed, academia should be creating more training materials based on projected industry needs. If creating cross-disciplinary graduates is a goal of higher-ed, then they need to set their expectations and pathways starting in middle school. This need for mixed skills in today's cybersecurity professionals is nothing new though since even in 2010 experts were demanding that cybersecurity students be taught not only technical skills but also have a baseline interdisciplinary understanding of formulating policies, risk management, navigating business standards, creating frameworks, governance, and much more [10, 23].

D. Invest In The NTTP Model

Industry, academia, and government should invest more into NTTPs, especially as an alternative to universities/colleges. Some of these NTTP programs could cater more to neurodiversity, and the current organizations leading efforts to create more free training and pathways should be championed and emulated. Some examples are ISC^2 committing to provide free training to over a million people, CISA providing grant funding to two NTTPs working in underserved communities, SANS providing GIAC certification opportunities for students at HBCUs, etc. Academia should not feel threatened by NTTPs, since almost all of their other programs will follow the traditional training model. Instead, Academia should consider creating their own NTTPs just for cybersecurity and emerging technology skill development.

E. Apprenticeships

Industry should create fully remote summer apprenticeships for high school students that cater to underserved communities and those in the Digital Divide. A key aspect would be for these specific apprentices to get hands-on experience they likely wouldn't receive in a traditional internship. This would also allow the apprentice to better build career capital with a potential employer and determine if that organization is a good culture fit. This would require more thoughtfulness and preparation on the organization, which could receive free support and structure through the Department of Labor's Cybersecurity Apprentice Program. The return on investment outweighs the cost though, since getting eager cybersecurity/emerging technology professionals that can be grown into organizational leaders may help Digital Security departments and organizations stay competitive in the 2026-2028 market.

F. Mentoring

Allow for mentoring of young professionals and higher-ed students with small groups of high school/middle school students instead of one-on-one. Give workplace incentives to young professionals and credits to higher-ed students who participate. For NTTP students, allow small tuition reductions for mentoring commitment and/or make mentoring part of the program. Keep it as small groups and allow monitoring to ensure mentorship programs from industry, government, and students in higher-ed working at high school/middle school STEM programs. Adults and volunteers would need to be vetted for skills, receive ethics training, and be screened for risky social behavior. There were recommendations among the workgroups for mid to senior-level professionals to mentor middle/high school kids which could be done, but that has inherent social risks and would likely be less beneficial to the students. A small group of high school seniors being mentored by a young professional in their first few years of a career is more relatable than senior professionals in the twilight of their career. That is not to say young students wouldn't benefit from a senior mentor, only that creating programs relying on young professionals instead of senior ones will likely produce more benefits for the profession. Training would need to be undergone before adults work in school to cover ethics, responsibilities, behavior expectations, and avoiding compromising situations.

G. Incentivize Teaching STEM

Middle/high school teachers should be incentivized instead of expected to go above and beyond in teaching STEM. Most teachers are already overworked and underpaid, and the current "free" training given to them too often has a paywall or is learning by PowerPoint. Professional training organizations that do good PBL are expensive and require expertise, which school and district leaders need to fight for. Leaders in education are ultimately responsible for all of the students at their school and need to present upward to districts and state representatives that the teaching of cybersecurity augmentation-related subjects is a non-partisan interest that deserves special treatment and resources. States then should request federal standards for the subjects of automation and cybersecurity, which need to be treated as non-partisan issues.

H. More Problem-Based Learning

The key action for initiating the above recommendations is to create more problem-based learning opportunities. Industry could sponsor and provide simplified resources that 7-12th grade teachers can use with students. Older Cyber Ranges and entry-level-cyber challenges could be a big part of this downward shift, with an emphasis on making content more engaging and informative. Government could allow students to conduct academic security audits, giving them experience and helping connect them to the needs of society. Academia could shift their STEM and higher-ed technology learning to PBL, requesting skill and work role mapping from industry to ensure they are teaching what's needed now and in the near future. Academia and industry could also begin working together specifically on taking already created Cyber Ranges/Challenges and repacking them for different learning levels. For example, K-6 (introduction to technology) could be more picture/game based, 7-9 (foundations in technology) introduces labs with video walkthroughs, 10-12 (securing technology) could be more game/video/lab-based with PDF walkthroughs, and higher-ed/NTTPs (becoming a professional of technology security) could use the same professional challenges accompanied with detailed walkthroughs.

VI. Conclusion

The NICE Conference brings together experts interested in sharing and learning what's working and what needs to happen with regard to cybersecurity education, training, career pathways, apprenticeships, and reskilling. It is pushing professionalization for government, industry, and academia in a way that must be expanded and adopted so cybersecurity can gain a single set of standards, norms, and development pathways. One major need for this to happen is for the NICE Framework and Conferences to have more operations and technical cybersecurity professionals participating in these future workforce discussions. Technical professionals must collaborate more with their workforce planners and developers for accurate and relevant career paths to be established. Planners of this workforce and those existing in this new type of ever-expanding profession must also find more ways to be transparent and collaborate across sectors while providing their needs to academia for refinement of curriculums.

Acknowledgment

The author would like to thank Jason Hite for co-hosting the event and Svea Anderson for her planning and onsite support. Panelist experts Anastacia Webster, Alibadi Roozbeh, and Athit Kao, PhD, were essential to creating the discussion that helped participants consider the role of emerging technologies in their current and future workforces. Finally, a special thanks to Florida International University for administering the NICE Conference and to Rodney Peterson for his leadership and vision in forwarding the professionalization of cybersecurity.

REFERENCES

[1] Bloom-Feshbach, A., & Poyet, M. (2018). The rise of digital team building. *People & Strategy*, *41*(2), 52-56. https://link.gale.com/apps/doc/A535943011/AONE?u=anon~e9dc0e26&sid=googleScholar&xid=bdf17200

[2] Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019). The role of artificial intelligence in cyber security. *Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems.* 170-192. IGI Global. https://doi.org/10.4018/978-1-5225-8241-0.ch009

[3] Brownlee, M. (2022, May 16). DALLE: AI made this thumbnail! [Video]. YouTube. https://www.youtube.com/watch?v=yCBEumeXY4A

[4] Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*. https://doi.org/10.48550/arXiv.1802.07228

[5] Dhillon, G., Smith, K., Hedström, K. (2019). Ensuring core competencies for cybersecurity specialists. *Cybersecurity Education for Awareness and Compliance* (121-133). IGI Global. https://doi.org/10.4018/978-1-5225-7847-5.ch007

[6] Dobson, S. (2018). Cybersecurity talent hard to find: Report. *Canadian HR Reporter, 31*(9), 3-18. https://www.hrreporter.com/focus-areas/recruitment-and-staffing/cybersecurity-talent-hard-to-find-report/299496

[7] Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security, 100*, 102080. https://doi.org/10.1016/j.cose.2020.102080

[8] Kallio, H., Pietilä, A.M., Johnson, M., & Docent, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing, 72*(12), 2949-3217. https://doi.org/10.1111/jan.13031

[9] Isberto, M. (2021). What is cybersecurity automation? *Colocation America.* https://www.colocationamerica.com/blog/cybersecurity-automation

[10] Jacob, J., Wei, W., Sha, K., Davari, S., & Yang, T. (2018). Is the Nice Cybersecurity Workforce Framework (NCWF) Effective for a Workforce Comprising of Interdisciplinary Majors? *16th International Conference on Scientific Computing, page 124-130.* https://par.nsf.gov/biblio/10095246

[11] Lippert, K. & Cloutier, R. (2021) Cyberspace: A digital ecosystem. *Systems 2021, 9*(3), 1-20. https://doi.org/10.3390/systems9030048

[12] Mackay, H., & Strickland, M. (2018) Exploring culturally responsive teaching and student-created videos in an at-risk middle school classroom. *Middle Grades Review 4*(1), 7. https://scholarworks.uvm.edu/mgreview/vol4/iss1/7

[13] Nobles, C. (2018a). The cyber talent gap and cybersecurity professionalizing. *International Journal of Hyperconnectivity and the Internet of Things. 2*(1), 56-63. http://doi.org/10.4018/IJHIoT.2018010104

[14] Nobles, C. (2018b). Botching human factors in cybersecurity in business organizations. *HOLISTICA – Journal of Business and Public Administration,9*(3), 71-88. https://doi.org/10.2478/hjbpa-2018-0024

[15] NAPA Workforce Report. (2022). A call to action: The federal government's role in building a cybersecurity workforce for the nation. *National Academy of Public Administration.* https://s3.us-west-2.amazonaws.com/napa-2021/studies/dhs-cybersecurity-workforce/NAPA-Final-CISA-Cybersecurity-Workforce-Report-January-2022.pdf

[16] NICE CON. (2022). Demystifying cybersecurity: Integrated approaches to developing career pathways. *NICE Conference and Expo 2022.* https://niceconference.org/wp-content/uploads/2022/06/NICE-2022-Program-Book.pdf

[17] NICE. (2020). *Cybersecurity NICE Framework.* National Institute of Standards and Technology. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

[18] Sadik, S., Ahmed, M., Sikos, L., Islam, A. (2020). Toward a sustainable cybersecurity ecosystem. *Computers* 2020, *9*(3) https://doi.org/10.3390/computers9030074

[19] Van Deursen, A., & Van Diik (2015). The digital divide shifts to differences in usage. *New Media & Society 16*(3), 507-526. https://www.doi.org/10.1177/1461444813487959

[20] Wang, P., Hayes, N., Bertocci, M., Williams, K., & Sbeit, R. (2020). The role of partnership and collaboration with cybersecurity industry in cyber defense education: A panel discussion. INTG Conference Las Vegas, June. https://www.researchgate.net/profile/raed-sbeit/publication/342425245_the_role_of_partnership_and_collaboration_with_cybersecurity_industry_in_cyber_defense_education_a_panel_discussion/links/5ef3b07a4585153fb1b38d66/the-role-of-partnership-and-collaboration-with-cybersecurity-industry-in-cyber-defense-education-a-panel-discussion.pdf

[21] Wetzel, K. (2021). *NICE Framework competencies: Assessing learners for cybersecurity work (Draft NISTIR 8355).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8355-draft

[22] Whitman, M. (2018). Industry priorities for cybersecurity competencies. *Journal of The Colloquium for Information Systems Security Education (CISSE), 6*(1). https://cisse.info/journal/index.php/cisse/article/view/91/CISSE_v06_i01_p06.pdf

[23] White, G., Williams, D., & Harrison, K. (2010). The CyberPatriot national high school cyber defense competition. *IEEE Security & Privacy, 8*(5), 59-61. https://doi.org/10.1109/MSP.2010.166

[24] Wong, G. K., Ma, X., Dillenbourg, P., & Huan, J. (2020). Broadening artificial intelligence education in K-12: Where to start?. *ACM Inroads, 11*(1), 20-29. https://doi.org/10.1145/3381884

[25] Yang, S., (2019). A curriculum model for cybersecurity master's program: A survey of AACSB-accredited business schools in the United States. *Journal of Education for Business, 16*(8), 520-530. https://doi.org/10.1080/08832323.2019.1590296

ABBRIVIATIONS AND ACRONYMS

ADHD – Attention Deficit Hyperactivity Disorder
AI – Artificial Intelligence
APTs – Advanced Persistent Threat Actors
CISA – U.S. Cybersecurity and Infrastructure Security Agency
DHS – U.S. Department of Homeland Security
GIAC – Global Information Assurance Certification
HBCUs – Historically Black Colleges and Universities
Higher-ed – All professional training post high school
ISC^2 – International Information System Security Certification Consortium
KSA – Knowledge, Skills, & Abilities
ML – Machine Learning
NICE – U.S. National Initiative for Cybersecurity Education
NIST – U.S. National Institute of Standards and Technology
NTTP – Non-Traditional Training Programs
ONCD – U.S. Office of the National Cyber Director
OPM – U.S. Office of Personnel Management
PBL – Problem Based Learning
RQ – Research Question
SANS – Escal Institute of Advanced Technologies
SME – Subject Matter Expert
STEM – Science, Technology, Engineering, Mathematics
TKS – Tasks, Knowledge, & Skills
TTPs – Tactics, Techniques, & Procedures