ISSN: 2473-4901
v8 n5760

# CyberEducation-by-Design

Paul Wagner
paulewagner@arizona.edu
Department Cyber, Intelligence, and Information Operations
University of Arizona
Tucson, Arizona

## Abstract

Most survey results agree that there is a current and ongoing shortage of skilled cybersecurity workers that places our privacy, infrastructure, and nation at risk. Estimates for the global Cybersecurity Workforce Gap range from 2.72 million to 3.5 million for 2021 and the United States' estimates range from 465,000 to over 700,000 open jobs as of September 2022. The most optimistic estimates still demonstrate a critical issue. Many approaches to this problem take a siloed approach of improving or introducing cybersecurity curriculum at a younger age, focus on point in time training and certification, or skills development through internships, apprenticeships, and work experience. Solving this problem requires an integrated approach that incorporates education, training and certification, and experience that is accessible to all, at any age or experience level. This paper will propose a CyberEducation-by-Design methodology and framework. This methodology and framework is based on a review of current government initiatives and legislation that recognizes and addresses the cybersecurity education and workforce development problem. Additionally, standards and curriculum available for K-12, Community and 2-Year Colleges, and 4-Year and beyond institutions will be outlined to cover the educational aspects of the problem. Further, skills development through certifications, On-the-Job-Training (OJT) and internships / apprenticeships, experiential learning, and work experience will be discussed.

**Keywords:** Cybersecurity Education, K-12 Education, Workforce Development, Certification

## 1. INTRODUCTION

The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy (Biden, 2021). This is evidenced by the recent Colonial Pipeline Attack (Turton, 2021); SolarWinds Attack (CIS, 2021); and ransomware attacks against healthcare systems (Weiner, 2021), U.S. schools and colleges (Kshertri, 2021) and critical infrastructure (Cluley, 2021). Most survey results agree that there is a current and ongoing shortage of skilled cybersecurity workers that places our privacy, infrastructure, and nation at risk. Estimates for the global Cybersecurity Workforce Gap range from 2.72 million (ISC2, 2021) to 3.5 million (Cyber Academy, 2021) for 2021 and the United States' estimates range from 465,000 (Brooks, 2021) to over 700,000 (Cyber Seek, 2022) open jobs as of November 2021. The most optimistic estimates still demonstrate a critical issue. Many approaches to this problem take a siloed approach of improving or introducing cybersecurity curriculum at a younger age, focus on point in time training and certification, or skills development through internships / apprenticeships, and work experience. The purpose of this paper is to propose a CyberEducation-by-Design Framework. This framework takes elements from various siloed initiatives to consolidate approaches that incorporates education, training and certification, and experience that is accessible to all at any age or experience level. Supporting this framework is a review of current government initiatives and legislation that recognizes and addresses the cybersecurity education and workforce development problem. Additionally, standards and curriculum available for K-12, Community and 2-Year Colleges, and 4-Year and beyond institutions will be outlined to cover the educational aspects of the problem. Further, skills development through certifications, On-the-Job-Training (OJT) and internships / apprenticeships, experiential learning, and work experience will be discussed.

## 2. PROPOSED WORK

### Research Design and Methodology

The author used a systematic literature review (SLR) technique to find relevant academic articles from 2010 to 2021. Relevant information was extracted from select articles to inform analysis and discussion. The steps involved in the SLR process include:

1. Define the research questions.
2. Determine the data sources and search process.
3. Inclusion and Exclusion Criteria.
4. Results of searching and data extraction.
5. Analysis and Discussion.

### Research Questions

1. What U.S. government legislation or initiatives have been developed to address cybersecurity education and workforce development?
2. What standards, curriculum, and initiatives have been introduced to address the cybersecurity and workforce development issues facing the U.S.?
3. What can be done to address the cybersecurity and workforce devolopment issues or improve upon current efforts?

### Data Sources and Search Process

A variety of sources were used to identify relevant sources for this research including Google Scholar, IEEE, Elsevier, EBSCO, Proquest and other library resources. Additionally, current industry trend reports were analyzed to identify current and relevant statistics to support research objectives. Search terms included but were not limited to linking the term "Cybersecurity" to Education, K-12 Education, Legislation, Dual Enrollment, Certifications, and Safety. The search limited results from 2010 to present.

### Inclusion and Exclusion Criteria

Given the limited, specific research on K-12 Cybersecurity education and its application to current cybersecurity workforce shortages, the author applied a liberal inclusive set of search criteria. Full-text journal articles were used to identify and analyze the current initiatives in cybersecurity education and training and current issues with cybersecurity workforce development. Information from these articles were extrapolated for their potential use in developing the CyberEducation-by-Design framework. Editorials, trade journals, and other online resources were used to identify the latest statistics, applications, and concerns facing cybersecurity education and workforce development.

### Search Results

Search results can be broadly categorized into cyber-safety, cyber-education, and cyber-skills. The table provided in Appendix A focuses on the efforts to address the cyber education and workforce development issues; however, supplemental and supporting references are provided in the reference section.

## 3. GOVERNMENT LEGISLATION

Arguably, "Cybercrime" and the need for cybersecurity professionals has been around for nearly two centuries when a pair of thieves hacked the French Telegraph System to steal financial market information in 1834 (Herjavec, 2019). Since that time, cybercrime and cyber warfare has become more commonplace and sophisticated. Despite this long need for cybersecurity professionals, it wasn't until President Reagan signed into law the Computer Security Act of 1987 directing the National Bureau of Standards to, "establish a computer standards program for Federal computer systems, including guidelines for security of such systems drawing on technical security guidelines developed by the National Security Agency (NSA)." (Glickman, 1988, p. 6). President Clinton established the President's Commission on Critical Infrastructure Protection in 1996 and released the first national strategy for protecting the nation's computer networks from attack in 2000 (Clinton, 2000).

In 2003, President Bush released The National Security Strategy to Secure Cyberspace which articulated five national priorities:

I. A National Cyberspace Security Response System,
II. A National Cyberspace Security Threat and Vulnerability Reduction Program,
III. A National Cyberspace Security Awareness and Training Program,
IV. Securing Governments' Cyberspace, and
V. National Security and International Cyberspace Security Cooperation (Bush, 2003).

Four major actions and initiatives tied to Priority III which directly relates to this paper include:

- Promote a comprehensive national awareness program to empower all Americans; businesses, the general workforce, and the general population, to secure their own parts of cyberspace,

- Foster adequate training and education programs to support the Nation's cybersecurity needs,
- Increase the efficiency of existing general cybersecurity training programs, and
- Promote private-sector support for well-coordinated, widely recognized professional cybersecurity certifications (Bush, 2003).

President Obama led many initiatives to improve the nation's cybersecurity. Briefly, these include the Cyberspace Policy Review (2009), making U.S. Cyber Command permanent (2009) (Armerding, 2013), issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity (2013)," which led to the National Institute of Standards and Technology (NIST) developing the Cybersecurity Framework (2014) (Obama, 2013), development of the Cybersecurity Act which includes Cybersecurity Information Sharing, National Cybersecurity Advancement, Federal Cybersecurity Workforce Assessment, and a variety of other cyber matters (2015) (Obama, 2015), and the implementation of the Cybersecurity National Action Plan (CNAP) which established the Commission on Enhancing Cybersecurity, modernize government IT, empower Americans to secure their online accounts (CNAP, 2017). CNAP enhanced cybersecurity education and training, through the National Initiatives for Cybersecurity Education (NICE) to expand Scholarship for Service opportunities, develop a cybersecurity core curriculum, and strengthen the National Centers for Academic Excellence in Cybersecurity Program.

President Trump issued Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which focused on modernizing federal information technology infrastructure, working with state and local government and private sector partners to more fully secure critical infrastructure, and collaborating with foreign allies (CISA, 2020). In response to this, The Department of Commerce and Department of Homeland Security investigated cybersecurity workforce development determining the following:

- The U.S. cybersecurity workforce needs immediate and sustained improvements,
- It is necessary to expand the pool of cybersecurity candidates through retraining and by increasing the participation of women, minorities, and veterans,
- There is a shortage of cybersecurity teachers at the primary and secondary levels, faculty in higher education, and training instructors, and
- Comprehensive and reliable data about cybersecurity workforce positions needs and education and training programs are lacking (CISA, 2020).

Most recently, President Biden issued his Executive Order to improve U.S. cybersecurity which focuses on removing barriers to threat information sharing between government and the private sector, improve software supply chain security, establish a cybersecurity safety review board, create a standard playbook for responding to cyber incidents, improve detection of cybersecurity incidents on federal government networks, and improve investigative and remediation capabilities (Biden, 2021). Additionally, the K-12 Cybersecurity Act of 2021 was signed into law ordering CISA to conduct an analysis of how cybersecurity risks specifically impact K-12 educational institutions, conduct an evaluation of the challenges K-12 educational institutions face in securing information systems and student records and implementing cybersecurity protocols, identifying cybersecurity challenges relating to remote learning, and evaluate the most accessible ways to communicate cybersecurity recommendations and tools (Cybersecurity Act, 2021).

## 4. STANDARDS ORGANIZATIONS

Several standards organizations are involved in overcoming the cybersecurity workforce gap in response to or in support of these government initiatives. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-181, Workforce Framework for Cybersecurity (National Initiatives for Cybersecurity Education (NICE) Framework), provides a set of building blocks for describing the tasks, knowledge, and skills (TKS) that are needed to perform cybersecurity work performed by individuals and teams for employers, education and training providers, and learners (Petersen, 2021). The NICE Framework attempts to define the TKSs in generic terms that can be applied to all organizations and are agile, flexible, interoperable, and modular (Petersen, 2021). The NICE Framework is comprised of seven categories of common cybersecurity functions which are broken down into 33 specialized areas that have defined Knowledge, Skills, and Abilities (KSAs) to complete defined tasks for that specialized area. Additionally, Capability Indicators for Entry, Intermediate, and Advanced roles across training, experiential learning, education, continuous learning, and credentials / certifications are defined. These items provide the building blocks for a Capable and Ready Cybersecurity Workforce (Figure 1).

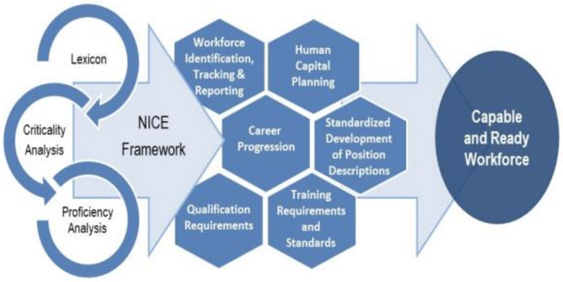

Lexicon
Criticality Analysis
Proficiency Analysis
NICE Framework
Workforce Identification, Tracking & Reporting
Human Capital Planning
Career Progression
Standardized Development of Position Descriptions
Qualification Requirements
Training Requirements and Standards
Capable and Ready Workforce

**Figure 1: Building Blocks for a Capable and Ready Workforce (Newhouse, 2017)**

The National Security Agency's (NSA) Cryptologic School manages the National Centers of Academic Excellence in Cybersecurity (NCAE-C). NCAE-C is supported by multiple federal partners to create and manage a collaborative cybersecurity educational program with community colleges, colleges, and universities that:

- Establish standards for cybersecurity curriculum and academic excellence,
- Includes competency development among students and faculty,
- Values community outreach and leadership in professional development,
- Integrates cybersecurity practice within the institution across academic disciplines, and
- Actively engages in solutions to challenges facing cybersecurity education (NCAEC, N.D.)

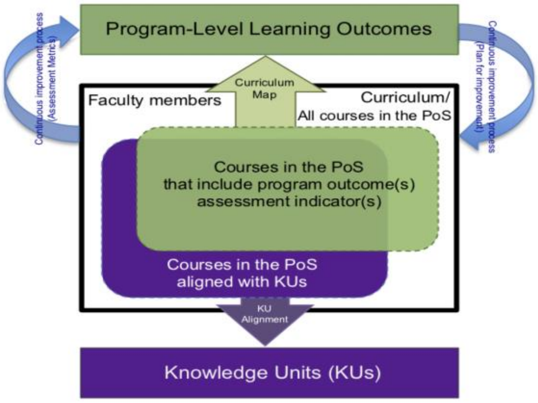

Program-Level Learning Outcomes
Continuous improvement process (Assessment Metrics)
Continuous improvement process (Plan for improvement)
Curriculum Map
Faculty members
Curriculum/ All courses in the PoS
Courses in the PoS that include program outcome(s) assessment indicator(s)
Courses in the PoS aligned with KUs
KU Alignment
Knowledge Units (KUs)

**Figure 2: NCAE-C Program of Study (PoS) Evaluation Conceptual Model (NCAEC, 2021)**

Academic institutions may be awarded one of three designations based on various criteria: Cyber Defense, Cyber Research, and Cyber Operations. These academic institutions align their curriculum map to learning outcomes which align with the NIST / NICE Framework. Additionally, the NCAE-C requires that designated programs integrate a continuous improvement process to ensure that the curriculum evolves with the state of cybersecurity outlined in Figure 2.

## 5. CURRICULUM

The National Cybersecurity Training and Education (NCyTE) Center aims to advance cybersecurity education in the U.S. by investing in technological innovation, resources, professional development, and tools to support faculty, community colleges, and the workforce pipeline of tomorrow (About NCyTE, 2021). NCyTE provides resources for faculty, industry, and centers of academic excellence. Additionally, NCyTE provides cybersecurity curriculum consisting of dozens of modules across a variety of topics including Advanced Placement Computer Science Principles; Cybersecurity, Cyber Intelligence Curriculum, Critical Infrastructure Security & Resilience (CISR), Critical Infrastructure Cybersecurity, Applied Cryptography, Cyber Threats & Counter Measures, Responsible Software Development, Secure Scripting, Cybersecurity and Society, Cybersecurity Principles, and Securing Data From Risk (Cybersecurity Curriculum, 2021). NCyTE supplements this content by providing webinar series, workshops, and resources to run camps and other activities.

Similarly, Cyber.org's goal is to empower educators as they prepare the next generation to succeed in the cyber workforce and ensure that every K-12 student receives foundational and technical cybersecurity knowledge and skills (Cyber.org, 2021). Cyber.org released the first national K-12 cybersecurity learning standards focused on computing systems, digital citizenship, and security. Cyber.org has thousands of hours of curriculum broken down by grade level across career and technical education, computer science, cybersecurity, engineering, humanities, math, robotics and coding, and science. Additionally, cyber.org provides professional development to empower educators.

Two additional resources for obtaining and sharing resources and curriculum are the Centers of Academic Excellence in Cybersecurity Resource Directory (CARD) (CARD, 2021) and the Cybersecurity Labs and Resource Knowledge Base (CLARK) (CLARK, 2021) to support educational institutions. CARD is a general resource directory that contains reports, grant deliverables, conference resources, competition frameworks, workshops and materials, and additional resources to support labs and summer camps. CLARK is focused on the development and sharing of cybersecurity curriculum. Content is broken down by topic (22 topic areas), education level (Elementary-, Middle-, High-School, Undergraduate, Graduate, Post-Graduate, Community College, and Training), and length (Nanomodule – 1 hour or less, Micromodule – 1 – 4 Hours, Module – 4 – 10 Hours, Unit – Over 10 Hours, Course – 15 Weeks) (CLARK, 2021).

## 6. CURRENT SOLUTIONS

The developed curriculum and support by the U.S. government appears to support solving the cybersecurity education and workforce development problem. NIST / NICE and NCAE-C outline standards; and NCyTE, Cyber.org, CARD, and CLARK provide hundreds of hours of curriculum, content, workshops, and webinars to empower educators. Despite this, the cybersecurity education and workforce development problems continue to exist. There are a few reasons for this. First, focused cybersecurity education and training mostly begins at the collegiate level and is siloed. Second, industry does not know what KSAs they need for the roles they are trying to fill. This is evident by job ads where skills, position levels, and pay are incongruent. Finally, aligning with the movement of cybersecurity education into the K-12 space, "Cyber-Safety" must be implemented seemingly at birth considering that internet connected toys and devices enter children's lives early. This section outlines previous work that addresses Cyber-Safety, Cyber-Education, and Cyber-Skills designed to improve capabilities of the cyber workforce and reduce risk.

### Cyber-Safety

Cyber-Safety initiatives can reduce the nation's susceptibility to cybercrime and reduce risk. Cyber criminals typically prey on the weakest or most vulnerable; therefore, steps must be taken to educate and prepare those systems and populations at the greatest risk. Cyber-Safety is applicable to everyone. People are introduced to technology at different points of their lives and their fluency with technology depends on many factors. Cyber-safety should be introduced at a young age considering technology will be part of their entire lives. Children are taught how to safely navigate their world from a young age. This includes how to safely cross the street, not touching sharp or hot objects, wearing protective devices like helmets and seat belts, fire safety, stranger safety, and water safety. The research, content, and application of cyber-safety for children birth to 5 years remains under researched and limited in practice (Edwards, 2021). Additionally, the long term impacts of identity theft with this population may not be understood for years.

Similarly, the elderly population, those aged 65 years or more, are at increased risk. Cybercrime against elderly fits into two general categories of fraud committed by strangers targeting investments, charity contributions, and loans and mortgages and financial exploitation by relatives and caregivers (Arfi, 2013). According to the FBI (Munanga, 2019), older adults are prime candidates of these crimes due to their credit history and when cognitive decline necessitates the need for others to manage their finances. This cohort typically lacks the familiarity with technology that other generations have. Additionally, they are less likely to be cognizant of cybersecurity threats and lack the experience to identify fraud in the digital space. The Center for Internet Security (Aliperti, 2021), Cyber Patriot CyberGenerations Program (Cyberpatriot 2022), the Cybersecurity & Infrastructure Security Agency (CISA, 2022), and various industry and government partners offer training and resources to support the elderly. Despite the increased awareness, training, and available resources; the financial damage for seniors is estimated at $1.68 billion annually (Abbate, 2021).

### Cyber-Education

As previously mentioned, there are seven common cybersecurity functions and 33 specialized areas as defined in the NICE Framework. These areas span from the non-technical to the deeply technical. Additionally, individuals from all backgrounds leverage cyber resources during daily life. Thus, Cyber-Education content must be tailored to the audience. Research conducted at Southeastern Louisiana University determined that survey participants not in a technology-focused major are at a disadvantage when it comes to general cybersecurity knowledge and privacy practices (McNulty, 2021).

Similarly, Cyber-Education must be integrated into all education levels. The curriculum must be tailored to be digestible and applicable for each age / education level. This requires a multi-level, multi-discipline approach that provides a level of cybersecurity education that is appropriate for an individual's role in society as depicted in Figure 3.

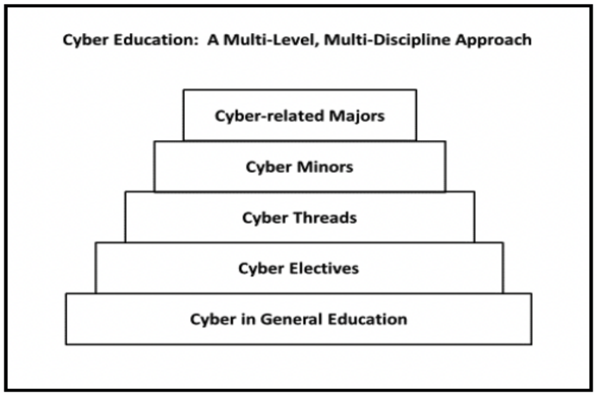

Cyber Education: A Multi-Level, Multi-Discipline Approach
Cyber-related Majors
Cyber Minors
Cyber Threads
Cyber Electives
Cyber in General Education

**Figure 3: Multi-Level, Multi-Discipline Cyber Education Approach (Sobiesk, 2015)**

Additionally, cybersecurity educational programs vary in content, application, breadth and depth, and integrated labs with hands-on learning. The work of NICE, NCyTE, Cyber.org, and others seeks to ensure that graduates at various levels have the tangible skills necessary to secure and thrive in the cybersecurity profession. Additionally, there are approximately 80 CAE-R, 22 CAE-CO, and over 200 CAE-CD designated schools (CAE, 2021). These schools meet or exceed the requirements set by the National Security Agency and are reviewed by peer institutions to ensure consistency and quality across schools.

Further, cybersecurity education programs focusing on high school students are being developed. Regions Investing in the Next Generation (RING) is an online high school cybersecurity course that offers content for students and schools without existing cybersecurity programs which will officially launch in 2022 (RING, 2022). RING allows students to achieve high school credit in participating states. Also, RING provides networking and professional development through the RING student organization. Additionally, Cyber.org facilitated collaboration among key stakeholders to develop and publish a set of K-12 cybersecurity learning standards. These standards center on computing systems, digital citizenship, and security to ensure that students have a foundational understanding of cybersecurity and the skills and knowledge to pursue cybersecurity careers (Cyber.org, 2022).

## Cyber-Skills

People starting their cybersecurity careers have three primary methods for developing skills necessary to increase employability. These are learning skills through self-study or other experiential learning, completing industry certifications, or gaining a related degree (Marquardson, 2018). This section focuses on the complementary skill development of certifications, On-the-Job Training (OJT) and Internships / Apprenticeships, and experiential learning.

### *Certifications*

Research indicates that certifications are important since they build confidence in cybersecurity professionals, validate their level of knowledge and skills versus untrained employees, and can execute their assigned tasks more consistently (James, 2019). Since 1989, Information Technology certifications have been introduced to reinforce and assess individuals or groups (Jarocki, 2019). Certifications are generally broken down into vendor-neutral and vendor-specific. Certification vendors factor in the current threat landscape, changing technologies, workforce needs, industry standards, and government and regulation to develop and maintain the certifications depicted in Figure 4.

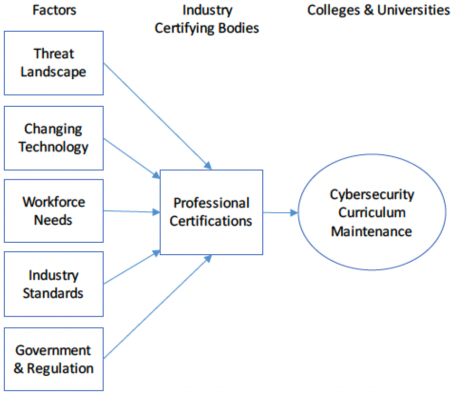


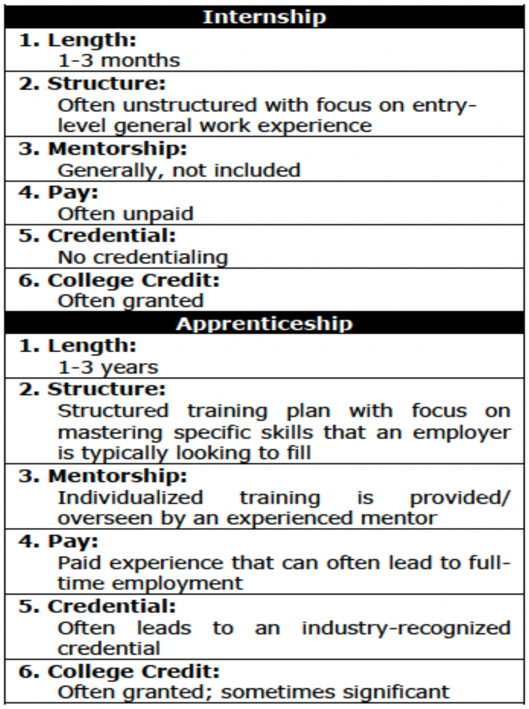
**Figure 4: Factors Impacting the Maintenance of Cybersecurity Certifications (Knapp, 2017)**

There are hundreds of cybersecurity certifications provided by many organizations including Computing Technology Industry Association (CompTIA), International Council of Electronic Commerce Consultants (EC-Council), Global Information Assurance Certification (GIAC), ISACA, and the International Information Systems Security Certification Consortium (ISC2). The 2022 Cybersecurity Certification Roadmap (Jerimy, 2022) maps over 400 certifications across various cyber domains of Communication and Network Security, Information Assurance Management, Security Architecture and Engineering, Asset Security, Security and Risk Management, Security

Assessment and Testing, Software Security, and Security Operations. (Appendix B).

***On-the-Job-Training / Apprenticeships / Internships / Experiential Learning***

Cybersecurity degree programs obtain a competitive advantage based on the amount of "hands-on" content within the curriculum considering industry requires a significant amount of skills-based training (Glantz, 2021). Complementing this "hands-on" content embedded into education programs and certifications is On-the-Job Training (OJT), internships / apprenticeships, and experiential learning. Internships and apprenticeships allow potential employees to gain, develop, and refine their cybersecurity skills while providing insight into the career field. Access and value to these opportunities varies. Figure 5 outlines key differences between these two opportunities.



| Internship |
|---|
| **1. Length:**<br>1-3 months |
| **2. Structure:**<br>Often unstructured with focus on entry-level general work experience |
| **3. Mentorship:**<br>Generally, not included |
| **4. Pay:**<br>Often unpaid |
| **5. Credential:**<br>No credentialing |
| **6. College Credit:**<br>Often granted |
| **Apprenticeship** |
| **1. Length:**<br>1-3 years |
| **2. Structure:**<br>Structured training plan with focus on mastering specific skills that an employer is typically looking to fill |
| **3. Mentorship:**<br>Individualized training is provided/ overseen by an experienced mentor |
| **4. Pay:**<br>Paid experience that can often lead to full-time employment |
| **5. Credential:**<br>Often leads to an industry-recognized credential |
| **6. College Credit:**<br>Often granted; sometimes significant |

**Figure 5: Internship and Apprenticeship Differences (Stoker, 2021)**

Although the experiences vary, the results are positive considering those that complete at least one internship receive 16% more job offers than those who don't and 94% of individuals that complete an apprenticeship program retain employment (Goin, 2021).

Finally, experiential learning in the form of self-study, participating in summer camps, and participating in "capture-the-flag" competitions can augment other skill development opportunities. For example, the Air Force Association (AFA) sponsored CyberPatriot program has evolved from a defense based cybersecurity competition to include curriculum to support elderly (Cybergenerations), educators (Elementary School Cyber Education Initiative (ESCEI)), and an information campaign through their CyberPatriot Literature Series. The CyberPatriot National Youth Cyber Defense competition challenges teams of high school and middle school students to find and fix cybersecurity vulnerabilities in virtual operating systems (CyberPatriot, 2021). Alternatively, the GenCyber program provides cybersecurity experience for students and teachers at the secondary level. GenCyber focuses on:

- Increasing awareness of K-12 cybersecurity content and career opportunities,
- Increase student diversity in cybersecurity college and career readiness pathways, and
- Facilitate teacher readiness within a teacher learning community (GenCyber, 2022).

Additionally, the National Cyber League (NCL) bridges the gap between high school and college students by providing a performance-based, learning-centered cybersecurity competition providing practical cybersecurity challenges competitors are likely to face in the workplace (NCL, 2021). Alternatively, TryHackMe (TryHackMe, 2021) and HacktheBox (HTB, 2021) provide platforms for gaining hands-on cybersecurity skills.

## 7. A BETTER APPROACH

As previously stated, a unified approach incorporating the various learning opportunities must be developed to solve the cybersecurity workforce problem. An example is the Cross-Boundary Cyber Education Design (Glantz, 2020) which builds upon the Multi-Level, Multi-Discipline Cyber Education Approach by adding curricular design insights from cyber master's degree programs and cyber certification offerings (Figure 6).

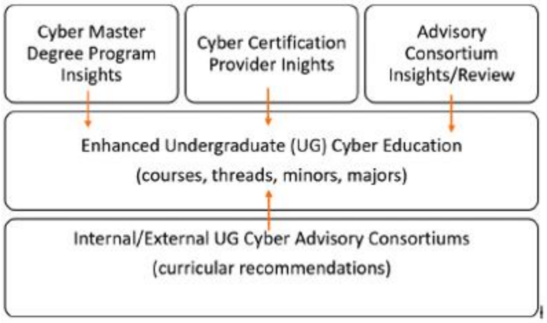

Cyber Master Degree Program Insights
Cyber Certification Provider Insights
Advisory Consortium Insights/Review
Enhanced Undergraduate (UG) Cyber Education
(courses, threads, minors, majors)
Internal/External UG Cyber Advisory Consortiums
(curricular recommendations)

**Figure 6: Cross-Boundary Process Guiding Undergraduate Research (Glantz, 2020)**

Although a more inclusive view of developing undergraduate education, it still does not include K-12 education and cyber safety. Additionally, government initiatives, legislation, and regulation can drive or limit innovation in the education space. This must be considered.

A "CyberEducation-by-Design" approach should be developed to incorporate the various components previously discussed from: cyber-safety, cyber-education, and cyber-skills. This should include the following key components:

- Curriculum designed and applicable to the age group and appropriate for the individual's roles in society.
- Curriculum designed to be accessible and inclusive. This may include Diversity, Equity, and Inclusion (DEI), socio-economic status of the individual and the school district, and several factors.
- Individuals should be able to inject themselves into the cybersecurity talent pipeline at any point. Many incoming cybersecurity professionals transfer from other careers, upskill within Science, Technology, Engineering, and Math (STEM) fields, or find non-traditional paths to cybersecurity.
- A holistic approach incorporating safety, education, certifications, and experiential learning should work synergistically to remove silos.
- When possible, clearly articulated pathways should be developed.

Figure 7 maps these various aspects grounded in standards based curriculum at various grade levels. Depending on the school and school district, the titles and age ranges for the various school levels may vary slightly. The center of the diagram is focused on the educational levels and associated age groups at those educational levels. The elements above the educational aspects integrate safety concepts, camps, and competitions accessible at those ages / educational levels. The elements below focus on experiential learning and skill development aligned with workforce development.

The Cybersecurity Education Pathway Table provided in Appendix C demonstrates a pathway that maps cybersecurity curriculum and certifications from a high school to an associated community college to a four-year institution. For the purposes of this mapping, general education courses are not included. Additionally, the experiential learning aspects outlined in this paper can be programmed into the curriculum to support learning objectives and skill development.

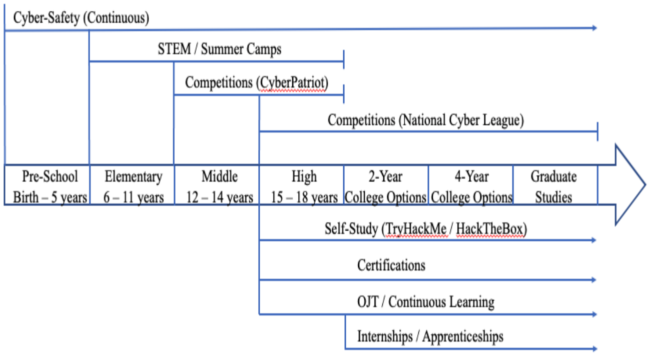

Cyber-Safety (Continuous)
STEM / Summer Camps
Competitions (CyberPatriot)
Competitions (National Cyber League)
Pre-School
Birth – 5 years
Elementary
6 – 11 years
Middle
12 – 14 years
High
15 – 18 years
2-Year
College Options
4-Year
College Options
Graduate
Studies
Self-Study (TryHackMe / HackTheBox)
Certifications
OJT / Continuous Learning
Internships / Apprenticeships

**Figure 7: CyberEducation-By-Design Model**

This course sequence and pathway is based on an existing pathway from Basha High School's Institute of Cyber Operations and Networking (Basha, 2022), Chandler Gilbert Community College's Associate of Applied Science in Cybersecurity (CGCC, 2022), and the University of Arizona's Cyber Operations program (Cyber Operations, 2022). The pathway provides a seamless educational experience through the educational levels. Opportunities for mentorship, camps, experiential learning, professional development, internships, and employment are integrated throughout. These opportunities are provided by local, state, and national partners.

## 8. CONTRIBUTIONS

Contributions of this paper include (1) a historical review of government legislation that recognize and attempt to address cybersecurity education and deficiencies within the cybersecurity workforce, (2) an outline standards organizations including NIST / NICE and NCAE-C, and (3) an outline of the available curriculum provided by NCyTE, Cyber.org, CLARK, and CARD. Additionally, a systematic literature review was conducted to identify initiatives being implemented to address the cybersecurity education and workforce development problem. This review focused on cyber-safety, cyber-education, and cyber-skills. Most importantly, a "CyberEducation-by-Design" approach was introduced. This design maps various aspects of cybersecurity education and training holistically. This model will require further refinement and additional overlays can be introduced and integrated to improve upon the initial design. Specifically, extending the timeline beyond graduate studies or branching a pathway for non-traditional learners could enhance the model. Additionally, articulated pathways can aid students in selecting cybersecurity as a career and understand their options earlier.

## 9. LIMITATIONS AND FUTURE RESEARCH

Multiple curriculum resources were discussed in this paper. The focus was on vetted, open source resources that are general enough to allow for adoption by a variety of education institutions. This represents a fraction of the overall free and open source content available and does not include content provided by textbook publishers or paid content. Future research in this area could be more inclusive of these options and potentially map all resources available to provide a central repository for that information. CLARK and CARD attempt to do that but is limited in scope and scale.

The concepts of internship and apprenticeship were integrated into the CyberEducation-by-Design model; however, building those opportunities requires significant effort. Additionally, directly integrating job opportunities into the model and developing a reliable "Cradle to Grave" approach where every cybersecurity program leads to employment and continuous learning. These may be provided by or integrated into the organizational culture of government and industry partners. Developing repeatable internship and apprenticeship opportunities could be the focus of future research.

Finally, funding was not explored in this study. There are many grant and scholarship opportunities for educators, students, curriculum development, and developing and hosting experiential learning opportunities. These range from individual awards to consortiums of multiple schools. Cataloguing these opportunities and making them accessible to stakeholders can address or improve many of the issues associated with cybersecurity education and workforce development discussed in this paper.

## 10. CONCLUSIONS

There continues to be hundreds of thousands of unfilled jobs within the United States and millions globally. Additionally, adversaries are rapidly building their cyber capabilities both in numbers and skills. Further, -as-a-Service capabilities allow adversaries to quickly execute attacks with limited or no preparation. Overcoming these things requires a holistic, agile, and innovative approach adopted by students, educators, employers, and governments.

Since President Reagan signed the Computer Security Act of 1987, presidents have taken a proactive stance on addressing the nation's cybersecurity issues through improved legislation including the National Security Strategy to Secure Cyberspace, Executive Order 13636 "Improving Critical Infrastructure Cybersecurity", implementing the Cybersecurity National Action Plan, Executive Order 13800 "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", the K-12 Cybersecurity Act, and others. These actions led to the development of NIST Special Publication 800-181 Workforce Framework for Cybersecurity (NICE Framework) and the NSA's National Centers of Academic Excellence in Cybersecurity (NCAE-C) standards. Additionally, in partnerships with these agencies and others, free and open source curriculum has been developed and catalogued by NCyTE, Cyber.org, CARD, and CLARK. These initiatives provide a foundation for addressing this national problem.

The literature review identified initiatives to address the cybersecurity education and workforce development problem focusing on three categories including cyber-safety, cyber-education, and cyber-skills. Cyber-safety identified the need for early and ongoing safety campaigns to ensure that all citizens have the knowledge and skills necessary to operate within their societal roles. Additional focus should be on the most vulnerable cohorts: infants, toddlers, and the elderly. Cyber-education reviewed the need for well-defined cybersecurity functions and job roles mapped to the required knowledge, skills, and abilities to meet those functions. These requirements help define the curriculum content. Additionally, cyber-education must be integrated into all education levels at the appropriate level for the learner in a multi-level, multi-discipline educational approach. Further, curriculum across educational institutions can vary greatly. Ensuring that schools are evaluated and meet certain content and quality standards is important. Finally, cyber-skill development in the form of certifications, On-the-Job-Training (OJT), apprenticeships, internships, and experiential learning were discussed.

Finally, a "CyberEducation-by-Design" model was introduced to address the need for curriculum to be integrated at all levels across disciplines that is appropriate for the learner. This curriculum must be accessible and inclusive. It also acknowledges that aspiring cybersecurity professionals inject themselves into the talent pipeline at different points on the spectrum and points in their lives. Cyber safety, education, certifications, and experiential learning should work synergistically and when possible, clearly articulated pathways should be developed. Although improvements can be made to this model, developing a repeatable, inclusive, and comprehensive model can greatly improve the cybersecurity posture of the nation.

## 11. REFERENCES

"A Massive Hacking Playground," (2021). Hack The Box. https://www.hackthebox.com/.

Abbate, P. (2021). Federal Bureau of Investigation Internet Crime Report 2021. Internet Crime Complaint Center. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

"About NCyTE," (2021). National Cybersecurity Training and Edcuation Center (NCyTE) Center. https://www.ncyte.net/about-us/about.

"About Us" (2021). Cyber.org. https://cyber.org/about-us, 2021.

Aliperti, M. (2021, June). How to Protect Seniors Against Cybercrimes and Scams. Center for Internet Security. https://www.cisecurity.org/insights/newsletter/how-to-protect-seniors-against-cybercrimes-and-scams.

Arfi, N. and Agarwal, S. (2013, June). Knowledge of Cybercrime among Elderly. International Journal of Scientifica & Engineering Research. https://www.researchgate.net/profile/Shalini-Agarwal-5/publication/242654499_Knowledge_of_Cybercrime_among_Elderly/links/0deec51cebeac0feef000000/Knowledge-of-Cybercrime-among-Elderly.pdf.

Armerding, T. (2017, January 31). Obama's cybersecurity legacy: Good intentions, good efforts, limited results. CSO Online. https://www.csoonline.com/article/3162844/obamas-cybersecurity-legacy-good-intentions-good-efforts-limited-results.html.

Basha High School (2022). Institute of Cyber Operations and Networking. Basha High School Cybersecurity Academy. https://www.cusd80.com/BHSCyber.

Biden, J. (2021, May 12). Executive Order on Improving the Nation's Cybersecurity. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Brooks, K. (2021, May 21). U.S. has almost 500,000 job openings in cybersecurity. CBS News. https://www.cbsnews.com/news/cybersecurity-job-openings-united-states/.

Bush, G. (2003, February). The National Strategy to Secure Cyberspace. A White House Report. https://ciaotest.cc.columbia.edu/olj/gli/gli_nov2003/gli_nov2003k.pdf.

"CAE Institution Map," (2021). CAE In Cybersecurity Community. https://www.caecommunity.org/cae-map.

GCGG (2022). Associate in Applied Science in Cybersecurity. Chandler-Gilber Community College. https://www.cgc.edu/degrees-certificates/computer-and-information-technology/cybersecurity-3197-aas.

CIS (2021, March 15). The SolarWinds Cyber-Attack: What You Need to Know. Center for Internet Security. https://www.cisecurity.org/solarwinds/.

CISA (2020, October 28). Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastrucutre. Cybersecurity & Infrastructure Security Agency (CISA). https://www.cisa.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure.

Clinton, B. (2000, February 16). President Clinton: Working to Strengthen Cybersecurity. The White House, White House at Work. https://clintonwhitehouse4.archives.gov/WH/Work/021600.html.

Cluley, G. (2021, October 21). US Government warns of BlackMatter ransomware attacks against critical infrastructure. Tripwire. https://www.tripwire.com/state-of-security/security-data-protection/us-government-warns-of-blackmatter-ransomware-attacks-against-critical-infrastructure/.

Cyber Academy (2021). Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021. Cyber Academy. https://cyberacademy.co/cybersecurity-talent-crunch-to-create-3-5-million-unfilled-jobs-globally-by-2021/.

Cyber Innovation Center and Cyber.org (2021). K-12 Cybersecurity Learning Standards. https://cyber.org/sites/default/files/2021-10/K-12%20Cybersecurity%20Learning%20Standards_1.0.pdf.

Cyber Operations (2022). Bachelor of Applied Science in Cyber Operations. University of Arizona. https://cyber-operations.azcast.arizona.edu/.

CyberPatriot (2022). CyberGenerations – The Senior Citizens' Cyber Safety Initiative. Air Force Association. https://www.uscyberpatriot.org/Pages/Special%20Initiatives/CyberGenerations-Overview.aspx#:~:text=CyberGenerations%20%2D%2D%20the%20Senior%20Citizens,of%20a%20self%2Dpaced%20guide.

"CyberPatriot National Youth Cyber Education Program Competition Overview," (2021). Air Force Association. https://www.uscyberpatriot.org/competition

/Competition-Overview/competition-overview.

"Cybersecurity Curriculum," (2021). NCyTE Center. https://www.ncyte.net/resources/cybersecurity-curriculum.

Cybersecurity & Infrastructure Security Agency (2022). CISA Cybersecurity Awareness Program Older American Resources. CISA. https://www.cisa.gov/publication/cisa-cybersecurity-awareness-program-older-american-resources.

Cyber Seek (2022, September 9). Cyber Seek Cybersecurity Supply and Demand Heat Map. Cyber Seek. https://www.cyberseek.org/heatmap.html.

"Cybersecurity Education Resource Directory," (2021). National Cryptologic Foundation. https://www.caeresource.directory/home.

"Cybersecurity Labs and Resource Knowledge-base," (2021). Clark Center. https://clark.center/home.

Edwards, S. (2021, June 14). Cyber-safety and COVID-19 in the early years: A research agenda. Journal of Early Childhood Research. https://journals.sagepub.com/doi/pdf/10.1177/1476718X211014908.

"FACT SHEET: Cybersecurity National Action Plan." (2016, February 9). Office of the Press Security, The White House. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

GenCyber (2022). Inspiring the Next Generation of Cyber Stars. GenCyber. https://www.gen-cyber.com/about/.

Glantz, E., Bartolacci, M., Naseredding, M., and Fusco, D. (2020). Cross-Boundary Cyber Education Design. SIGTE. https://doi.org/10.1145/3368308.3415374.

Glickman, D. (1988, January 8). H.R. 145 – Computer Security Act of 1987. Congress.gov. https://www.congress.gov/bill/100th-congress/house-bill/145.

Goin, A., Branter, C., Johnston, L., Rodriguez, R., and Hott, J. (2021). Idaho Cyber Heroes: Helping Individuals Navigate Career Pathways in Cybersecurity. Idaho National Laboratory. https://inl.gov/wp-content/uploads/2021/09/3-CyberLeague-Whitepaper-Final-20210903.pdf.

Herjavec, R. (2019, July 17). Cybersecurity CEO: The History of Cybercrime, From 1834 to Present. Cybercrime Magazine. https://cybersecurityventures.com/cybersecurity-ceo-the-history-of-cybercrime-from-1834-to-present/.

ISC2 (2021). A Resilient Cybersecurity Profession Charts the Path Forward, ISC2 Cybersecurity Workforce Study, 2021. International Information Systems Security Certification Consortium. https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.

James, J. and Callen, J. (2019, October). Cybersecurity Certifications Matter. Issues in Information Security. https://www.researchgate.net/publication/338805856.

Jarocki, S. and Kettani, H. (2019). Examining the Efficacy of Commercial Cyber Security Certifications for Information Security Analysts. International Conference on Information Systems Engineering (ICISE). https://www.researchgate.net/publication/338506367_Examining_the_Efficacy_of_Commercial_Cyber_Security_Certifications_for_Information_Security_Analysts.

Jerimy, P. (2022, August). Security Certification Roadmap 2022. Paul Jerimy. https://pauljerimy.com/security-certification-roadmap/.

"Join 500k other learning Cybersecurity with TryHackMe," (2021). Try Hack Me. https://tryhackme.com/.

"K-12 Cybersecurity Act of 2021," (2021, October 8). 117th Congress Public Law No: 117-47, https://www.congress.gov/bill/117th-congress/senate-bill/1917/all-info.

Knapp, K., Maurer, C., and Plachkinova, M. (2017, December 12). Maintaining Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. Journal of Information Systems Education. http://jise.org/Volume28/n2/JISEv28n2p101.html.

Marquardson, J. and Elnoshokaty, A. (2018). Skills, Certifications, or Degrees: What Companies Demand for Entry-level Cybersecurity Jobs. Information Systems Education Journal. https://doi.org/10.48009/3_iis_2018_193-201.

McNulty, M. (2021). Cybersecurity Education for Non-Technical Learners. Beadle Scholar. https://scholar.dsu.edu/cgi/viewcontent.cgi?article=1365&context=theses.

Munanga, A. (2019, January 11). Cybercrime: A New and Growing Problem for Older Adults. Journal of Gerontological Nursing. https://doi-org.ezproxy3.library.arizona.edu/10.3928/00989134-20190111-01.

"National Centers for Academic Excellence in Cybersecurity," (N.D.). National Security Agency / Central Security Service. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/.

"National Centers of Academic Excellence in Cybersecurity CAE 2021: Proposed Designation Requirements and Application Process for CAE Cyber Operations," (2021, March). National Security Agency / Central Security Service. https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-proposed_cae-co_designation_requirements.pdf.

Newhouse, W., Keith, S., Sribner, B., and Witte, G. (2017, August). NIST Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf, August 2017.

Obama, B. (2013, February 12). Cybersecurity – Executive Order 13636. The White House. https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/eo-13636.

Obama, B. (2015). H.R.2029-694 – Cybersecurity Act of 2015. Senate.gov. https://www.intelligence.senate.gov/sites/default/files/legislation/Cybersecurity-Act-Of-2015.pdf.

Petersen, R., Santos, D., Smith, M., Wetzel, K., and Witte, G. (2020, November). NIST Special Publication 800-181 Rev. 1, Workforce Framework for Cybersecurity (NICE Framework). National Institute for Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181r1.

RING (2022). Regions Investing in the Next Generation (RING). https://caecommunity.org/initiative/k12-ring#:~:text=What%20is%20RING%3F,without%20an%20existing%20cybersecurity%20program.

.

Sobiesk, E., Blair, J., Conti, G., Lanham, M., and Taylor, H. (2015, October 3). Cyber Education: A Multi-Level, Multi-Discipline Approach. SIGITE. http://dx.doi.org/10.1145/2656450.2656478.

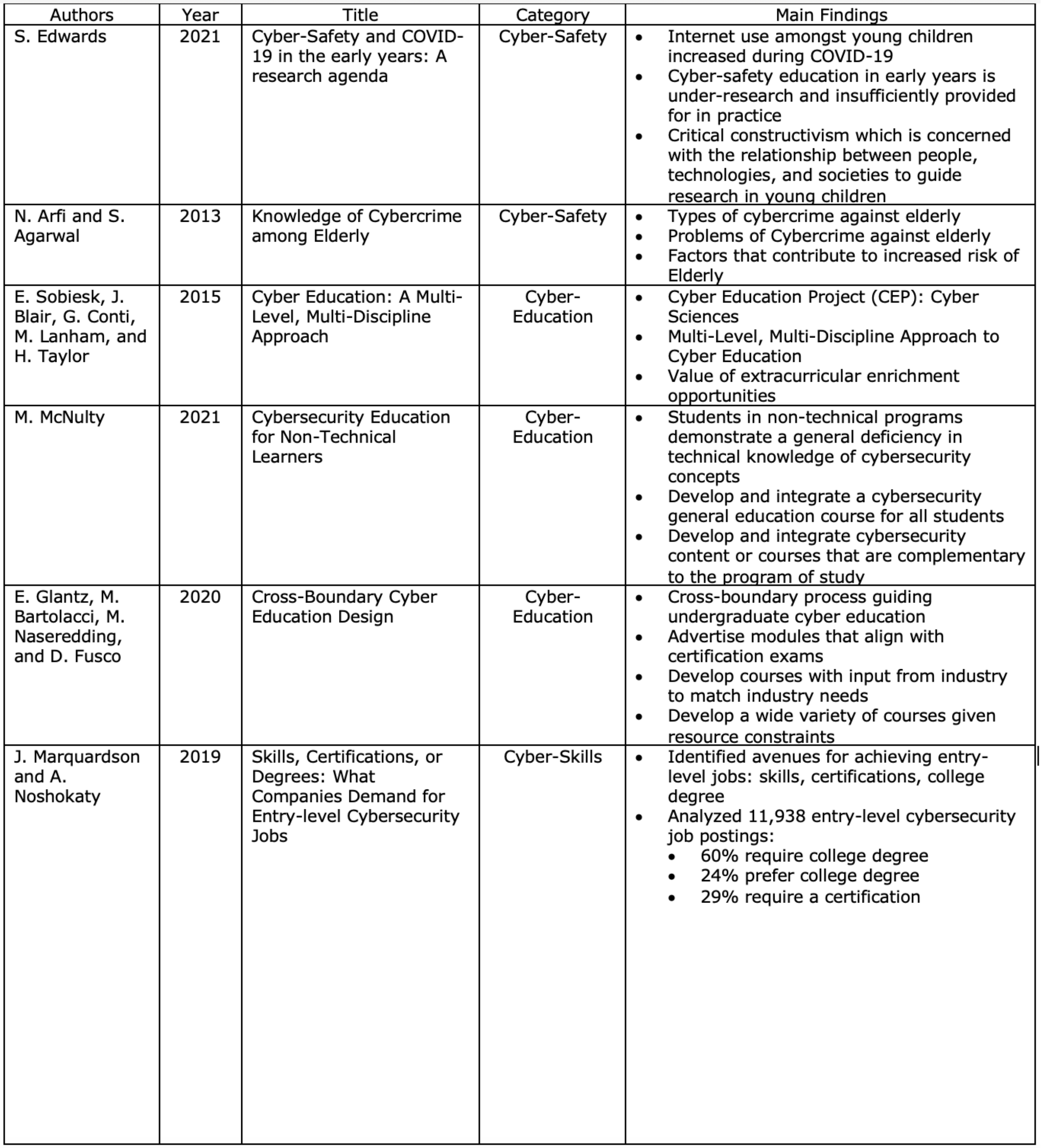
Stoker, G., Clark, U., Vanajakumari, M., and Wetherill, W. (2021, April). Building a Cybersecurity Apprenticeship Program: Early-Stage Success and Some Lessons Learned. Information Systems Education Journal (ISEDJ). https://files.eric.ed.gov/fulltext/EJ1297604.pdf.

"The National Cyber League," (2021). Cyber Skyline. https://nationalcyberleague.org/.

Turton, W. and Mehrotra, K. (2021, June 4). Hackers Breached Colonial Pipeline Using Compromised Password. Bloomberg Cybersecurity. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

Weiner, S. (2021, July 20). The growing threat of ransomware attacks on hospitals. Association of American Medical Colleges https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals

## Appendix A: Sytematic Literature Review Table

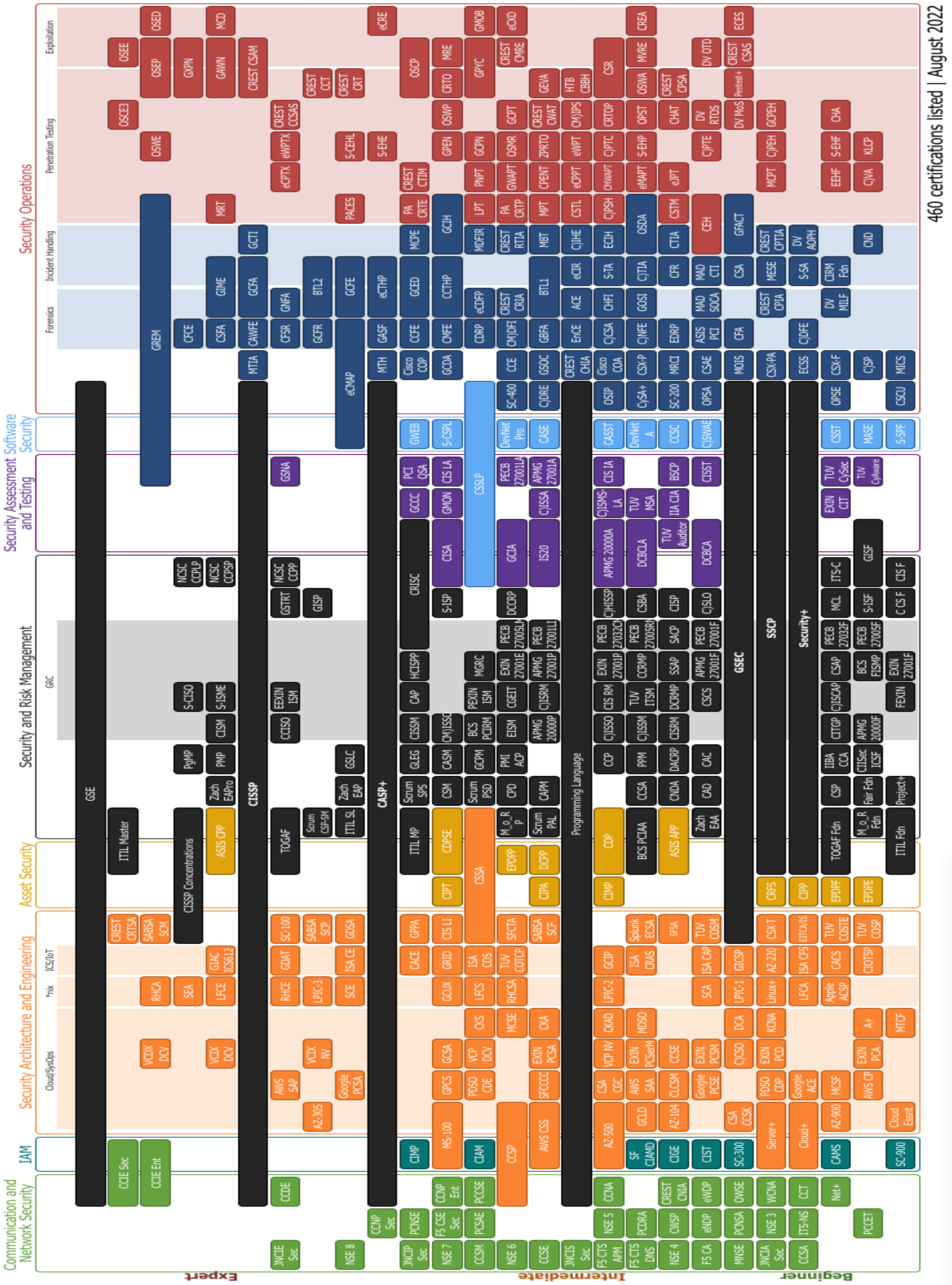


| Authors | Year | Title | Category | Main Findings |
|---|---|---|---|---|
| S. Edwards | 2021 | Cyber-Safety and COVID-19 in the early years: A research agenda | Cyber-Safety | • Internet use amongst young children increased during COVID-19<br>• Cyber-safety education in early years is under-research and insufficiently provided for in practice<br>• Critical constructivism which is concerned with the relationship between people, technologies, and societies to guide research in young children |
| N. Arfi and S. Agarwal | 2013 | Knowledge of Cybercrime among Elderly | Cyber-Safety | • Types of cybercrime against elderly<br>• Problems of Cybercrime against elderly<br>• Factors that contribute to increased risk of Elderly |
| E. Sobiesk, J. Blair, G. Conti, M. Lanham, and H. Taylor | 2015 | Cyber Education: A Multi-Level, Multi-Discipline Approach | Cyber-Education | • Cyber Education Project (CEP): Cyber Sciences<br>• Multi-Level, Multi-Discipline Approach to Cyber Education<br>• Value of extracurricular enrichment opportunities |
| M. McNulty | 2021 | Cybersecurity Education for Non-Technical Learners | Cyber-Education | • Students in non-technical programs demonstrate a general deficiency in technical knowledge of cybersecurity concepts<br>• Develop and integrate a cybersecurity general education course for all students<br>• Develop and integrate cybersecurity content or courses that are complementary to the program of study |
| E. Glantz, M. Bartolacci, M. Naseredding, and D. Fusco | 2020 | Cross-Boundary Cyber Education Design | Cyber-Education | • Cross-boundary process guiding undergraduate cyber education<br>• Advertise modules that align with certification exams<br>• Develop courses with input from industry to match industry needs<br>• Develop a wide variety of courses given resource constraints |
| J. Marquardson and A. Noshokaty | 2019 | Skills, Certifications, or Degrees: What Companies Demand for Entry-level Cybersecurity Jobs | Cyber-Skills | • Identified avenues for achieving entry-level jobs: skills, certifications, college degree<br>• Analyzed 11,938 entry-level cybersecurity job postings:<br>  • 60% require college degree<br>  • 24% prefer college degree<br>  • 29% require a certification |

| | | | | |
|---|---|---|---|---|
| J. James and J. Callen | 2018 | Cybersecurity Certifications Matters | Cyber-Skills | • Certifications matter: Confidence, Validation, Execution<br>• Cybersecurity certifications can increase KSAs and give students an edge when applying for jobs<br>• Co-curricular activities such as competitions, journals, webinars, and seminars can enhance KSAs |
| S. Jarocki and H. Kettani | 2019 | Examining the Efficacy of Commercial Cyber Security Certifications for Information Security Analysts | Cyber-Skills | • Value and Effectiveness of cybersecurity certifications<br>• Research is limited on efficacy of commercial incident response cyber security certifications in selecting potential candidates |
| K. Knapp, C. Maurer, and M. Plachkinova | 2017 | Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance | Cyber-Skills | • Factors impacting the maintenance of cybersecurity certifications<br>• Appropriateness of using certifications for curriculum shaping<br>• Experiential Learning and Capstone Courses |
| G. Stoker, U. Clark, M. Vanajakumari, and W. Wetherill | 2021 | Building a Cybersecurity Apprenticeship Program: Early-Stage Success and Some Lessons Learned | Cyber-Skills | • NICE Working Group on Apprenticeships<br>• Cyberstart Apprenticeship<br>• Cybersecurity Youth Apprenticeship Initiative |
| A. Goin, C. Branter, L. Johnston, R. Rodriguez, and J. Hott | 2021 | Idaho Cyber Heroes: Helping Individuals Navigate Career Pathways in Cybersecurity | Cyber-Skills | • Increasing Career Awareness in High Schoolers<br>• Requirements and Barriers for a Career in Cybersecurity<br>• Benefits of Internships and Apprenticeships<br>• Lack of Diversity in the Cybersecurity Workforce |

ISSN: 2473-4901
v8 n5760

## Appendix B – Certification Table



## Appendix C – Cybersecurity Education Pathway Table

| High School | Community College | 4-Year Institution |
|---|---|---|
| • Survey of Computer Information Systems<br>• Computer Hardware & Support*<br>• Operating System Configuration *<br>• Linux Operating System / Red Hat SysAdmin I<br>• Introduction to Networks<br>• AWS Cloud Foundations<br>• Linux SysAdmin / Red Hat SysAdmin II<br>• Information Security Fundamentals**<br>• Python Programming<br>• Ethics in Information Technology | • Ethical Hacking & Network Defense<br>• Computer Information Systems<br>• Internship / Special Project<br>• Computer Forensics Foundations<br>• Advanced Computer Forensics | • Computational Thinking & Doing<br>• Introductory Methods of Network Analysis<br>• Cyber Ethics<br>• Introduction to Cyber Operations**<br>• Active Cyber Defense<br>• Cyber Threat Intelligence<br>• Violent Python<br>• Cyber Threat Intelligence<br>• Cyber Warfare<br>• Additional Elective Course |
| * Maps to CompTIA A+ Certification<br>** Could map to Security+ Certification / Partial Preparation | | |