Journal of Cybersecurity Education, Research and Practice

Volume 2024 | Number 1 Article 20

4-29-2024

Cybersecurity Skills, Knowledge and Abilities for Criminal Justice Professionals: An Exploratory Study of Practitioners' Perspectives

Kate Quintana
University of Colorado Colorado Springs, kquintan@uccs.edu

Caroline Sutton Chubb
Georgia State University, cchubb1@student.gsu.edu

Daniel Olson
University of Colorado Colorado Springs, dolson@uccs.edu

Anna Kosloski
University of Colorado Colorado Springs, akoslosk@uccs.edu

Recommended Citation

Quintana, Kate; Sutton Chubb, Caroline; Olson, Daniel; and Kosloski, Anna (2024) "Cybersecurity Skills, Knowledge and Abilities for Criminal Justice Professionals: An Exploratory Study of Practitioners' Perspectives," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2024: No. 1, Article 20.
DOI: https://doi.org/10.62915/2472-2707.1175
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/20

Cybersecurity Skills, Knowledge and Abilities for Criminal Justice Professionals: An Exploratory Study of Practitioners' Perspectives

Abstract

Cybersecurity has become increasingly important not only in the technology sector but in criminal justice professions as well, and significant challenges have arisen as a result. However, these challenges are not well discussed in the literature. To address this gap, and to study the cybersecurity trends impacting criminal justice professionals and the skills, knowledge and abilities criminal justice students need to succeed upon graduation, this research focuses on the role cybersecurity plays in the jobs that compose the main components of the criminal justice system and adjacent areas: law enforcement, the judicial process, corrections, social work, and military. This research utilizes semi-structured interviews with current and recently retired practitioners. Findings from this study revealed eight broad themes, many of which are complementary including changing technologies, generational gaps, over reliance on information technology professionals, and best practices for education composed of experiential learning, soft skills, specialized curriculum and interdisciplinary approaches.

Keywords

Criminal justice education, cybersecurity, criminal justice profession

Cybersecurity Skills, Knowledge and Abilities for Criminal Justice Professionals: An Exploratory Study of Practitioners' Perspectives

Kate Quintana
College of Public Service
University of Colorado Colorado Springs
Colorado Springs, CO,USA
kquintan@uccs.edu
0009-0006-1865-6608

Caroline Sutton Chubb
College of Education and Human Development
Georgia State University
Atlanta, GA, USA
cchubb1@student.gsu.edu
0009-0005-9542-8492

Daniel Olson
College of Public Service,
University of Colorado Colorado Springs
Colorado Springs, CO, USA
dolson@uccs.edu
0009-0009-3157-6313

Anna E. Kosloski
College of Public Service,
University of Colorado Colorado Springs
Colorado Springs, CO, USA
akoslosk@uccs.edu
0000-0002-2373-4125

***Abstract*—Cybersecurity has become increasingly important not only in the technology sector but in criminal justice professions as well, and significant challenges have arisen as a result. However, these challenges are not well discussed in the literature. To address this gap, and to study the cybersecurity trends impacting criminal justice professionals and the skills, knowledge and abilities criminal justice students need to succeed upon graduation, this research focuses on the role cybersecurity plays in the jobs that compose the main components of the criminal justice system and adjacent areas: law enforcement, the judicial process, corrections, social work, and military. This research utilizes semi-structured interviews with current and recently retired practitioners. Findings from this study revealed eight broad themes, many of which are complementary including changing technologies, generational gaps, over reliance on information technology professionals, and best practices for education composed of experiential learning, soft skills, specialized curriculum and interdisciplinary approaches.**

Keywords—criminal justice education, cybersecurity, criminal justice profession

I. Introduction

As the world becomes increasingly digital, criminal justice organizations are tasked with the difficulty of balancing the use of technology with managing the risks of being connected in a virtual world. For example, in 2018 inmates at the Idaho Department of Corrections were able to hack prison tablets and steal approximately $225,000 of virtual credits [37]. This type of hack illustrates how even when incarcerated, cybercrime is occurring. As technology has become increasingly important in a globally interconnected world, it has also created new opportunities for criminal behavior and poses new challenges for how the criminal justice system responds to crime [29]. Further, computers and related technologies are increasingly the tools and targets of crime. Looking at cyber-attacks alone, Griffiths [12] estimates that there has been a global increase of 125% through 2021. Put together, this creates a large need for criminal justice professionals to know and employ sound cybersecurity practices [4;16]. According to the Cybersecurity and Infrastructure Security Agency, cybersecurity can be defined as: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation [24].

However, how those working in the criminal justice system understand and discuss cybercrime does not appear to be advancing as quickly as the technology used to facilitate it [31]. More specifically, criminal justice programs and career fields face considerable challenges regarding cybersecurity.

Starting with crucial knowledge before a profession begins, fields such as computer science and information technology have taken the lead on developing programs and practices concerning cybersecurity. However, criminal justice as a discipline lags behind. While the literature is just beginning to discuss how technology has been added to law enforcement policies, structure, and strategy, [7;20;44] there is still much to explore in the relationship between cybersecurity and criminal justice. Further, as Winger, Ellis, & Glover [45] note, there is a lack of discourse surrounding cybersecurity and curriculum. While Winger, Ellis, & Glover [45] explored how the gap lies in political science education, Nodeland, Belshaw, & Saber [25] note that same can be said for criminal justice education as well. Not only does this mean the relationship between criminal justice programs and cybersecurity is under-researched, but it

also means that there are few criminal justice programs that have fully embraced cybersecurity education.

The purpose of this exploratory research is to help educational institutions improve their criminal justice programs (1) by identifying cybersecurity trends impacting criminal justice professionals and (2) by articulating the cybersecurity skills, knowledge, and abilities that criminal justice professional need to succeed upon graduation. The current study focuses on cybersecurity in law enforcement, the judicial process, corrections, and cyber-adjacent fields by interviewing current and recently retired practitioners in each sector of the criminal justice system. Collectively, the interviewees provided broad perspectives that revealed several key lessons for students, academic institutions, and criminal justice practitioners at all levels of leadership.

II. LITERATURE REVIEW

A. Technical Knowledge

The increased reliance on technology means there are more threats of cybersecurity attacks and more opportunities for cybercrime [18]. Simultaneously, there is a shortage of cybersecurity professionals who may have the technical knowledge to prevent and respond to such threats [43]. As Johnson, Faulkner, Meredith, & Wilson [18] note, in a post-digital age, inexpensive digital technologies allow for a wide range of illicit behaviors in the virtual domain. Thus, the need for criminal justice personnel with new skills to understand, investigate and prosecute these behaviors is needed [27]. While the emerging literature tends to focus on the role of cybersecurity in law enforcement, other agencies within the criminal justice system are also vulnerable to cyber-attacks. Russo, Woods, Shaffer, & Jackson [34] reported correctional institutions spanning from small jails to large prisons face security threats as well. Upon concluding a workshop with prison officials, Russo, Woods, Shaffer, & Jackson [34] shared "correctional institutions are using more IT," however "they are generally failing to adequately manage cybersecurity risks to their systems, assets, and data" (p.13). These risks translate to vulnerabilities across communication and security platforms, health and safety software, and records about both staff and inmates.

In the context of criminal justice, Pfefferkorn [32] describes the use of deepfakes or artificial intelligence (AI) that allows for the creation of realistic but fake videos and images, highlighting the use of technology for harmful or criminal purposes. According to Pfefferkorn [32] deepfakes can be used to spread misinformation and may pose problems for attorneys in the courtroom. Additionally, courts hold valuable case data which can make them targets for cyber threats. Since COVID-19, the increased use of virtual courtrooms around the globe has heightened the need for the protection of information systems within judicial organizations [22].

As technology has advanced, the technical knowledge of job requirements has increased drastically over the years [14;40]. Yet, not all jobs in cybersecurity involve deep technical knowledge, and discussions are occurring around the role civilian employees (as opposed to sworn) may play in some of these specialized criminal justice areas, such as cybersecurity [15]. Harkin & Whelan [13] interviewed 43 professionals in specialized cybersecurity police units and reported civilian experts in cybersecurity units could help improve police knowledge and skills, and provide valuable historical knowledge given that sworn employees often rotate out of units. While police officers recognize the need to investigate cybercrime, Senjo [36] discovered that officer perceptions of cybercrime were guided by popular media depictions, stereotypes, and differed from scholarly literature on the topic. Similarly, Nouh, Nurse, Webb, & Goldsmith [27] interviewed cybersecurity investigators and found that one of the greatest challenges this population experiences is either miscategorizing cybercrimes which may result in either a lack of appropriate details or misdirecting a case to the wrong unit within an agency. A second critical challenge that Nouh, Nurse, Webb, & Goldsmith [27] found among their participants was that those with technical experience in police agencies are gaining employment in the broader cyber field. Collectively, these studies indicate a need to educate, train, and retain professionals with the skills and knowledge to adequately investigate cybercrimes and/or prevent and detect cyber-attacks on criminal justice agencies.

B. Soft Skills

Soft skills, or non-technical skills, have been identified by employers as critical for graduates entering the workforce. However, a mismatch exists between the skill of recent graduates and the expectations of employers [38;39]. El Messaoudi [10] points out that soft skills have become increasingly necessary as a part of education and contribute to the employability of college graduates globally. Further, soft skills are commonly listed in job competencies, and can be evaluated for prospective employees. Rios, Ling, Pugh, Becker, & Bacall [33] conducted a content analysis of roughly 142,000 online job postings to investigate skills considered critical for students' transition from higher education, and found that collaboration, problem solving, communication skills, critical thinking, ethics, and cultural sensitivity are commonly mentioned, with communication being the most requested skill across different disciplines. The focus on soft skills, particularly communication and human behavior, is also addressed by Chowdhury & Gkioulos [6] in a systematic literature review of the key competencies needed for critical infrastructure cybersecurity protection. This is backed by previous research recording an increase in employers in the informational technology field looking for individuals with communication and interpersonal skills [19]. More recently, Dawson & Thomson [9] highlight that in cybersecurity, end users are a major vulnerability, stressing the importance of soft skills and an interdisciplinary approach to cyber security work. This supports that criminal justice programs with a focus in cybersecurity must also be concerned with the training of students on soft skills, including communication in both written and oral forms, among other capabilities.

C. Interdisciplinary Education

Interdisciplinary approaches in education expose students to a variety of perspectives and encourage critical thinking in complex contexts. This is of importance in criminal justice education, particularly when considering the many fields in

which criminal justice professionals operate, as well as the diverse population criminal justice professionals serve. One example of cybersecurity interdisciplinary approaches can be found in Payne, He, Wang, Wittkower, & Wu [30], who created a general education course looking at cybersecurity through an interdisciplinary lens, highlighting fields that overlap and benefit from knowledge of cybersecurity, including through a criminal justice paradigm. Interdisciplinarity contains the promise of better understanding of relations between different fields of knowledge, and of how knowledge produced in the academy moves into society [8]. However, more discussions are needed about the potential of interdisciplinary approaches in the branches of criminal justice education, particularly in fields adjacent to cybersecurity. This echoes other research [9;28;17] that suggests that the development of a cybersecurity curriculum and workforce should consider many disciplines.

D. Education and Recruitment Gaps

There is an "extreme" global shortage of cybersecurity professionals reaching as high as 3 million [2;21;42]. The 2020 Cybersecurity Workforce Study found that employment in the field needs to grow by 41% in the United States and 89% worldwide to fill this gap [43]. This scarcity in talent does not exclusively affect cybersecurity-specific organizations. In fact, as Furnell [11] asserts, there is no sector that is not reliant upon cybersecurity and cybersecurity professionals. This has led to the widespread problem of finding qualified personnel to fill the required roles and duties as they relate to cybersecurity in modern organizations around the world. Further, newer, younger employees are undoubtedly more cyber-savvy than older workers, a bridge that must be addressed if our criminal justice agencies are to be secure and effective organizations. Ackerman [1] posits that no cybersecurity professional over the age of 30 has a degree in cybersecurity, but we cannot leave the burden of filling this gap to the generation under 30. Further, although not specific to criminal justice, prior job experience was mentioned in 84% of job ads for IT professionals, and this is not something that seems to be adapting to fit a younger, less formally experienced generation [19].

The challenge of addressing the shortage in cybersecurity professionals begins with a gap in education. Cybersecurity is a constantly changing field, and educational programs, oftentimes static in nature, are struggling to keep up [2; 26]. Further, there are active efforts in the European Union to collect data about cybersecurity offerings within educational programs to see how they match up with industry needs. As part of the UK cyber policy, cybersecurity knowledge is being implemented in all levels of educational programming starting at 11 years old [2]. However, in the United States, the closest program is the National Initiative for Cybersecurity Education (NICE), and they have found that educational programs are not providing individuals with skills necessary to acquire the knowledge needed for their positions in the workforce [2]. To our knowledge, NICE has not assessed the recruitment and education gaps of cybersecurity within criminal justice programs. Conversely, looking at a developing country with a stated elementary level of cybersecurity education, a study conducted with leading Ecuadorian educators demonstrated that a lack of specialization of professors and low availability of professors were some of the leading causes for the shortage of cybersecurity programs [5]. In 2011, the Centers for Academic Excellence examined where the 73 institutions that had a cybersecurity concentration or minor were housed, and only one was within a criminal justice program in the United States [28].

E. Gaps in Research

Although there is quite a bit of literature concerning informational technology, information systems, and cybersecurity, there is a dearth of research on the role these fields play in criminal justice. Additionally, given the rapidly changing nature of cyber, the research, like education, has lagged behind field advancements. While it is difficult to find mentions of criminal justice programs in prior cybersecurity research, publications specifically looking toward the future of cyber are more likely to acknowledge the need for cybersecurity education and training in criminal justice. For example, assessing what cybersecurity education will look like in 2030, Parrish, Impagliazzo, Raj, Santos, Ashgar, Josang, Pereira, & Stavrou [28] specifically point to cybersecurity as being one of the important subsets of criminal justice education.

III. METHODS

The current exploratory study presents interview data (n=9) focused on identifying cybersecurity trends impacting criminal justice professionals and articulating the cybersecurity skills, knowledge, and abilities that criminal justice professionals need to succeed upon graduation. Given the interdisciplinary nature of criminal justice, participants were recruited from law enforcement, the judicial system, corrections, the military, and social work. The sample was based on convenience as participants were identified through the team's network of contacts in two different states. While the sampling strategy was one of convenience, it was purposive in that all participants had to have (a) experience in the field, (b) extensive knowledge of, or direct participation in, the hiring process within their agency, and (c) an ability to speak to trends in cybersecurity as it impacts their agency. In this study, participants had between 10-30 years of experience and were either currently employed or recently retired. Demographic characteristics were not collected for the confidentiality of the participants.

Participants were emailed with an overview of the project aims and upon agreeing to participate in the study, completed the informed consent prior to data collection. A semi-structured interview design was utilized where participants were asked a series of questions related to the significance of cybersecurity within their organization, skills and knowledge that would be applicable to their agency and profession, and future directions for cybercrime and cybersecurity. Interviews were conducted by at least 2 members of the 4-person research team between September and November 2021. Interviews ranged from 45-60 minutes and were conducted using a videoconference tool. Each interview was audio-recorded, transcribed verbatim, and the data was de-identified to protect confidentiality.

Pseudonyms were generated with artificial intelligence to help reduce bias in assigning fictitious names.

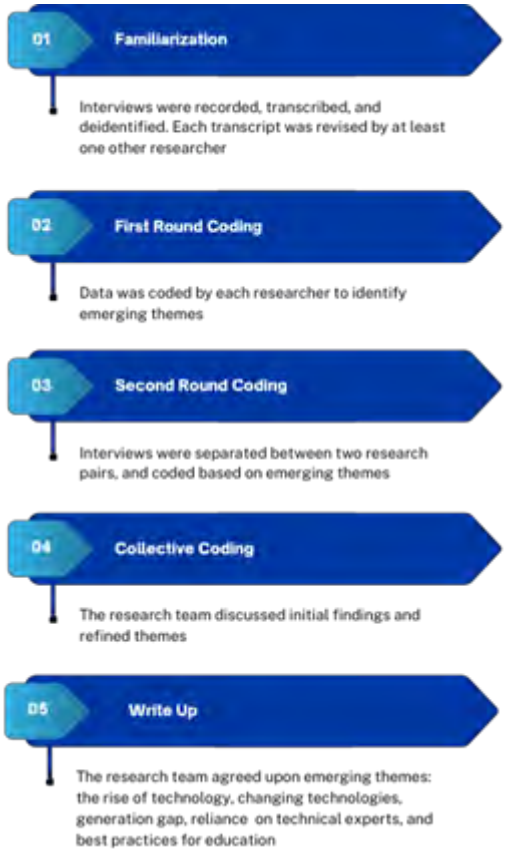
This study was exploratory in nature given the dearth of research about cybersecurity skills necessary in the criminal justice field. Thus, existing literature was used to help understand the current state of cybersecurity and cybercrime within criminal justice, and questions were developed to explore what criminal justice programs may want to incorporate into their curriculum to address skills and knowledge needed based on the changing nature of the criminal justice field. Questions were developed as part of a larger study; therefore, the current research utilizes answers to seven primary questions (see Table I) and the follow-up prompts (why, can you please provide an example, etc.) that were utilized to address the current study's aims.

TABLE I. SAMPLE QUESTIONS FOR PROFFESIONALS

1.	How important is cybersecurity in your organization?
2.	How important is it for recent college graduates newly employed in your organization to have a working knowledge of cybersecurity?
3.	Moving on to a related topic, how important is it for recent college graduates newly employed in your organization to have a working knowledge of cybercrime?
4.	In considering cybercrime and cybersecurity, what specific skills should students have?
5.	Are there specific programs or tools we should teach our students to use?
6.	Are there "gaps" between what you need from college grads and what universities are producing?
7.	What cybercrime or cybersecurity issues is your agency most focused on today?

Thematic analysis was utilized to identify themes and patterns within the interview data [3]. Data was coded by the four researchers based on emerging themes and themes could be coded into more than one category. After emerging themes were agreed upon by the researchers, a coding grid was created, and two researchers coded each transcript. Coding was then compared between the researchers to ensure interrater reliability. Data was considered reaching saturation as outlined in the a priori thematic approach by Saunders, Sim, & Kingstone [35] where data saturation is reached based on "the degree to which identified codes or themes are exemplified in the data" (p.1897). In this case, the researchers decided data saturation was reached because the same themes were consistent within the data. The analysis resulted in 8 core areas of focus, including: the rise of technology, changing technologies, generation gap, reliance on technical experts, and best practices for education (including soft skills, specialized curriculum, interdisciplinary focus, and experiential learning). The stages of this process are described in Table II

TABLE II. THEMATIC ANALYSIS STEPS



IV. RESULTS

A. *Emerging Trends & Challenges in Cybersecurity and Cybercrime within CJ*

The Rise of Technology. Our findings highlight that today's criminal justice professionals may take computers and related technologies for granted. Today's law enforcement officials, attorneys, and corrections officials are comfortable using computers, smartphones, tablets, and related technologies daily. However, this wasn't always the case. Across the board, participants stressed that computers and technology have become increasingly important in their respective fields. Participants repeatedly emphasized that technology will only continue to rise in importance, requiring increased technological savvy and an increased focus on cybersecurity and digital forensics.

In fact, Elizabeth, a recently retired public defender with over 30 years of criminal justice experience, stated that, "when I started as a public defender, we didn't even have computers […] you used a typewriter to do everything." In contrast, in today's world, Elizabeth highlighted the importance of data extraction, understanding cyberspace, and being able to explain cyber-related topics to juries. Similarly, in law enforcement, Maxwell, a detective with more than 20 years of experience as a uniformed police officer, highlighted that today, most criminal investigations involve the use of computer technology, particularly video recordings. In corrections, Sebastian reported that when he started twenty-five years ago, all records were simply kept in a written notebook. Similarly, Alexia, a

social worker whose clinical experience dates back to 2008, reported that the rise of tele-health and electronic records have resulted in an increased focus on cybersecurity in the social work community, a focus that did not exist a generation ago.

Rapidly Changing Technologies. Interviewees also highlighted that technological tools in the field are constantly changing at a rapid rate, leading to an inherent challenge for criminal justice programs and on-the-job-training programs alike. Relevant technologies may be different by the time the learner enters the career field to apply the technology. Maxwell explained, with a focus on the data extraction tools used in digital forensics, that:

[T]he mainstream tools are all really good to have knowledge of. The problem [is that we] train somebody up, and then next year, that tool is not as relevant, because it's constantly changing… So it'd be kind of hard to say, yes, [teach] this tool or yes [teach] that tool and stick with it (Maxwell).

The rapid rate of technological change has also posed a challenge for cybersecurity educators in military training and education programs. As Gabriel, a veteran with over 25 years of military service, noted, one solution currently in practice is working "very closely with a large sector of where our workforce actually works when they leave here [and continuing] to interface with them". Thus, as technologies evolve, curriculum is updated with a goal of "ensuring that our students are getting current, relevant education on the knowledge, skills, abilities and tasks that they're going to need when they move to their operating force." As will be discussed, one solution for higher education is to focus on internships in which students learn to use and apply cutting-edge technologies currently in use in criminal justice career fields. Interfacing with changing technologies and exposing students to these changes could better prepare them for the realities of the workforce.

Generational Gap. As previously discussed, the field of cybersecurity and technology is one that changes rapidly. The participants in this study noted how this leads to a generational gap in the workforce. This has led the experts to worry that we may be relying on individuals from younger generations, the ones who are believed to have grown up with, and are comfortable working with, advanced technology. They posit that these are the individuals that are assumed to take the many available cyber positions upon graduation. However, in the experience of our participants, it is a mistake to assume that these younger individuals both understand technology and are interested in pursuing a career related to technology. For example, as Henry, a retired military officer with over 30 years of service, stressed,

I think there is a general misconception by a lot of, say, older folks, that the generation that is still in training and in school – whether it's middle school, high school, or university – that they get cyber, they understand it, right, and so we don't have to worry because if we can just hold on a for a couple of years, they'll be in the workforce and everything will be fine and I couldn't disagree more.

Reliance on Experts. Another common theme that emerged in the data was the need for foundational knowledge in cybersecurity. For most study participants, it was clear that having basic knowledge of cybercrime and cybersecurity could help working professionals know what questions to ask when taking on a case with a cyber component. For example, Marina, a social worker since 2003, shared,

[As a social worker], if you're working on a case with somebody, you should at least have that background [on whether it involves] a cybersecurity crime. […] If you don't have that working background knowledge, then how would you be able to determine what the mitigating factors are? [For example], if you're looking at what type of punishment the DA should be going for, but you have no working knowledge of what the offense is or what the crime is, and how did this all come about. I think you have more of a problem of actually doing a full and complete picture for your job.

The sentiment of having a basic understanding of cybercrime and cybersecurity was shared largely across the field. Sebastian, who did not feel a basic understanding of cyber was necessary in the field of corrections, explained that it is not a primary focus for the profession. As Sebastian shared, basic training on cybersecurity would not be essential because "[the agency] provide[s] some basic training that gets us by, again, not much of our work is sort of geared towards addressing it […] I don't think [cybersecurity] would be a huge demand." Yet, for most participants, basic knowledge of cybersecurity and cybercrime was recognized both as a means of understanding cases that one might be working but also as a means to help protect client information and the organization from external threats:

If you come in ignorant of you know, just basic cybersecurity concepts, vulnerabilities, your learning curve is going to be steep right off the bat. So yeah, I think, I guess the way I would put it is: if we are not looking for people with those capabilities now, we're doing it wrong (William).

When we talk about establishing this culture of cybersecurity, that means everybody needs to be aware, because if you look at how the adversary actually exploits our networks, it's through individual people that make mistakes, we can have the best security posture in the world with cloud security, your own firewall defense in depth. But if that one person clicks on the one link in the email, then all of that great security is all for not. So you need to train people to not do that (Gabriel). While participants consistently talked about the value of recent graduates and employees in their fields having a basic understanding of cybercrime and cybersecurity, they noted a lack of training from their organizations on cybercrime and cybersecurity. For those that had training, this typically ranged from monthly or annual meetings focusing on being cautious of which emails are opened through agency computers and what phishing attempts may look like. This is shared across fields, including in law enforcement, where:

We have monthly security awareness trainings, it's just short, little few minute training on 'here's an example of what could happen if you get this e-mail or if you found this thumb drive', just more security awareness on your day-to-day job (Maxwell).

Again, the [agency name], requires us to do certain very simple, quick kind of trainings. …You know … I'll get an e-mail [and] it's something that looks pretty legit. It's not. I click on it and then boom, now I've been outed, and my name will go to somebody and then my chief [talks] to me that I didn't practice good, safe security. So, it keeps us on our toes. Nobody's getting in any trouble. But it's an awareness piece (Sebastian).

Most participants indicated that IT departments within the organization address external threats. Maxwell, representing a law enforcement perspective, shared that when it comes to a cyber intrusion "we're not that involved with that initial response – that would be our IT department that would be responsible for responding to something like that as it pertains to the [agency]." Similarly, when the professionals are working on a criminal case involving a cybercrime, if they do not have the technical experience within the agency, they often seek outside support.

A common refrain in cybersecurity career fields is that cybersecurity is not just an "IT issue" but an enterprise-wide issue. Training and education can be key pillars of success by ensuring that criminal justice professionals understand that cybersecurity is an issue that impacts everyone and is a responsibility of everyone, not just the technical experts. For example, Miranda [23] found that it is the frontline officers who need formal and practical cybersecurity training when it comes to their daily tasks such as managing and downloading body warn camera footage.

B. Identified Skills and Knowledge Needed for Future CJ Professionals

Whether explicitly or not, all of the experts expressed views on how education can better prepare students for cybersecurity roles in criminal justice. Their views centered around improving soft skills such as written and verbal communication, specialized curriculum such as specific courses and concentration areas, interdisciplinary approaches including the incorporation of other fields like psychology, and experiential learning or internships.

Soft Skills. When asked about the specific skills that students should have, the interviewees overwhelmingly mentioned skills that fall within the realm of soft skills such as problem solving, written and verbal communication and critical thinking. One individual discussed the importance of soft skills in retelling the experience of one of the students he had worked with, who was very competitive with his technical expertise but lacked communication skills. More specifically, reflecting on a 25-year military career, highlighted a common mismatch between academic and employment-based skills:

We had one of our cybersecurity graduates interview for one of the digital forensic investigator positions. And they were off the charts on the technical side. They had experience, they had additional certifications that they had done on their own…and then they went [to the] interview and… they were really lacking in those one-on-one communication skills. If you think of a digital forensic investigator, they have to go testify in court. And so if they're unable to communicate, you know, to the judge or to a jury, they're not going to be effective. So lesson learned was: okay, we need to go back and, even if you don't do an internship, we need to build…soft skills -- I just call them foundational, human skills – and prepare students so when they graduate, they're ready to go. And not only interview well but operate in some type of organizational environment and be successful.

Specialized Curriculum. Across participants, it was evident that including basic knowledge of cybercrime, cybersecurity, and digital forensics could hold value for students interested in working in the criminal justice system. While some participants, especially in law enforcement and corrections, noted their employees would receive further training in an academy or on the job, most participants across sectors of the CJ system felt some foundational knowledge would be valuable. A theme that occurred across interviews was the significance of understanding how technology is used in crimes so that officers can document and potentially collect evidence that may not appear relevant. As interviewees noted:

So just basic computer knowledge would be very helpful as well. As far as from like a digital forensics standpoint, you know we end up teaching most of that, or almost all of it once we get a person, but a lot of times what we'd be looking for from an officer who might want to apply to a unit such as this is experience with not only like using a computer, but can you fix a computer? Are you familiar with the hardware? Do you know how the different components interact inside? Do you know how networks work? Which then goes and decipher security because we have to secure our stuff in here separate from… (Maxwell).

Now the technology piece is still very important. I'm not trying to and I think if someone had a background in cybersecurity, they probably head up some of our initiatives locally when we're doing those trainings and they probably serve on a state committee. And so there'd be a lot of value added having that (Sebastian).

In addition to benefits for a variety of criminal justice professions, participants also noted that having some basic knowledge of cybersecurity, cybercrime, and/or digital forensics would make applicants more appealing in the application process. For example,

I think I would be really intrigued and I'd want to learn more about them. I think that would provide an advantage over maybe another candidate just because not because of

cybersecurity so much, but just that they would be, I think to me be more familiar with computer systems and be less intimidated by, you know, new computer programs …. every time they roll out a new system…. (Sebastian).

It would be helpful in that it's not required, but it demonstrates a higher level of commitment and makes the applicant more appealing (Jordan).

I think other beneficial things would be some of these classes; you know, taking some specialized classes I think would make you a better candidate over somebody else (Elizabeth).

Interdisciplinary Approaches. The interviews also highlighted that criminal justice programs should provide students with opportunities for interdisciplinary learning with a focus on psychology, sociology, and cybersecurity. Participants in all sectors emphasized the importance of interdisciplinary approaches in criminal justice education. Opportunities for interdisciplinary learning include dual degrees, minors, focus areas/concentrations, and opportunities for required or elective courses in psychology, sociology, and cyber-related fields (networking, cybersecurity basics). On a smaller scale, participants noted that incorporating guest speakers or interdisciplinary content in criminal justice courses is a viable option as well.

Participants highlighted several reasons for the importance of interdisciplinary approaches in criminal justice. Starting with a law enforcement perspective, William highlighted the importance of dual degrees in criminal justice and psychology and criminal justice and sociology. In the context of corrections, a similar theme emerged. Sebastian stated in broad terms that criminal justice graduates working in corrections benefit from "anything that deals with human behavior [and] sociology." Moreover, in addition to psychology and sociology, given the rise of technology in criminal justice career fields, criminal justice programs should include opportunities for students to study cybercrime, cybersecurity, and digital forensics.

Having established the importance of interdisciplinary approaches in law enforcement, it's equally important for prosecutors and defense counsel to approach their professions in an interdisciplinary way. Conveying information to juries is a key responsibility in our court system. Elizabeth emphasized that courts need attorneys who can present highly technical digital evidence in ways that juries can readily understand. Elizabeth also echoed the themes of law enforcement and corrections participants in highlighting that legal professionals such as prosecutors and defense counsel should have an understanding of psychology, as many cases will hinge on defenses involving mental culpability.

Interdisciplinary approaches are important not only for criminal justice programs but for technical disciplines such as cybersecurity. Cybersecurity is often perceived as a technical pursuit housed in computer sciences or engineering departments. It is important, however, for cybersecurity programs to recognize the importance of interdisciplinary approaches. As Gabriel, a cybersecurity professional (and retired military officer), stated:

Because it's not technology alone that's attacking us, right? It's people using technology. And so there is definitely a psychological component. There is a sociological component, there's a legal component, and then there's technical component. In other words, cybersecurity professionals and law enforcement officials have a variety of technical tools at their disposal as they carry out their duties, but it's important to ensure such technologies are used lawfully. Therefore, cybersecurity professionals must have a basic understanding of legal limitations, at least enough to know when to seek legal counsel. The social work experts agreed that they, too, can benefit from interdisciplinary approaches. Simply put by Marina, students "need to be able to understand learning across the disciplines and being exposed to multiple disciplines as they prepare to go out in the working world."

Experiential Learning. Participants repeatedly emphasized the importance of experiential learning, focusing on internships and volunteer opportunities as best practices in higher education. Participants highlighted several reasons for the importance of experiential learning. First, participants stressed that classroom learning does not necessarily mean that students are able to apply concepts in a non-academic setting (the "real world"), and experiential learning helps bridge this gap. This theme was especially evident in comments by Jordan, a corrections officer, in describing recent criminal justice graduates: "They learn some theory in a textbook, but they haven't learned how to put it into practical application, so that may be the largest gap that the corrections would see."

Jordan cited case management skills as a concrete example of this learning "gap" and others agreed that case management skills are exceptionally difficult to teach and learn in the classroom setting. Jordan stated that students simply aren't "learning how to manage caseloads, and I don't know how you teach that." One solution would be implementing internship programs in a public defender's office, social work clinic, or other criminal justice setting characterized by case management responsibilities. Digital forensics represents another concrete example where experiential learning can make a key difference. Per William, higher education should provide ample experiential opportunities for "getting your hands dirty [in] a little bit [of] digital forensics type thing instead of just taking notes and watching PowerPoint. It's hard to do, but I think that's beneficial as well."

Given the benefits of experiential learning and the practicalities involved in establishing robust internship programs, it's important to note that volunteer opportunities may work well in conjunction with, or in some cases, in lieu of, traditional college-sponsored internships. In the context of corrections, for example, probation manager Sebastian highlighted that the probation office had not only a strong internship program but also a vibrant volunteer program:

We've got almost 2000 people in our volunteers/intern program. …It's really integral to the success of our agency. So we love interns. We love our volunteers, and we give a lot of extra points within our screening process for anyone that's completed an internship. It's not guaranteed, but they're highly likely to get an interview if they've completed an internship with us (Sebastian).

Sebastian's comments highlight yet another benefit of internships: they clearly enhance students' employment prospects with the agencies they intern with. Regarding potential employment, another important theme emerged. A second reason for the importance of experiential learning, particularly internships and volunteering, is that it helps students understand the nature of various criminal justice organizations before seeking to join those organizations more permanently. Criminal justice agencies encompass a broad variety of missions, and it's important that students understand the mission and values associated with those agencies. For example, Elizabeth, reflecting on the courts component of our criminal justice system, stated that when discussing experiential learning,

Internships [are] definitely number one on the list. I think it's important that you volunteer in a public defender's office. You need to understand exactly what we do and show that you're committed to the mission of the public defender system. … It's important to understand … what my job is compared to what a prosecutor's job is, and how it's so different from what a prosecutor does.

Representing law enforcement, a participant espoused similar sentiments:

So I would say that having any internship where it could be at any level, any level law enforcement. Where they get a chance to understand police operations and investigations and interviews and things like that… that's our bread-and-butter skill sets so that's first and foremost to me… I do think law enforcement internships are probably invaluable for brand new college graduates coming out. (William)

To sum up, interviewees repeatedly emphasized the importance of time management, caseload management, and understanding how things actually work, skills that are best gained through internships, hands-on activities, and other forms of experiential learning. Criminal justice programs should provide meaningful internship opportunities at each step of the criminal justice system: internships in law enforcement, the court system, and in the corrections system. Internships foster soft skills such as negotiation and case management skills, bridge the gap between the textbook and the real world, enhance employment prospects, and help students understand the mission of diverse criminal justice agencies. Where internships are not an option, strong community relationships should be forged and advocated for to promote volunteer opportunities for students. Finally, where possible, experiential learning should be made part of classroom activities.

V. DISCUSSION

Our exploratory study examined the role that cybersecurity knowledge, skills, and abilities play in the preparation, hiring and success of criminal justice students going into the criminal justice field. Overall, our interviews revealed the key themes of changing technologies, generational gaps, over reliance on information technology professionals, and best practices for education composed of experiential learning, soft skills, specialized curriculum and interdisciplinary approaches. From the information gathered on these themes, several takeaways were presented.

Our interviewees emphasized that cybersecurity and its role in criminal justice is much more than just ones and zeros. In fact, the criminal justice professionals repeatedly stressed the interdisciplinary nature of their work with cyber and how soft skills, rather than technical skills, would make for a successfully employed recent graduate. This is not to say that the interviewees didn't also need to have at least a basic cyber awareness, because they do. However, when referring to the technical knowledge required, our findings illuminated that students should be able to understand the technical side of cybersecurity, whether through a class, a minor/major, or a certificate, but more importantly, they need to be able to work with people from other disciplines and be able to communicate what they know effectively.

To tie the educational programs together with the employability of recent graduates, our findings show that in the stand-alone, minor, or certificate classes, instruction should increase its focus on soft skills to include written and oral communication. Our findings on this echo existing research that suggests the importance of soft skill training that matches employers' expectations of skills, knowledge, and abilities, needed in the field [33;34]. Educational institutions should also focus on interdisciplinary approaches in cybersecurity-related course offerings and programs. Specifically, consulting the literature, "cybersecurity solutions must take into account all perspectives - human, technical, legal, political, ethical, scientific, and economic" [30].

Furthermore, the most recent report shows that only one quarter of accredited Bachelor of Criminal Justice programs in the United States offer concentrations, most of them in corrections, law enforcement, forensics, and homeland security [41]. Our interviews suggest that a cybersecurity course or concentration would be a competitive advantage in hiring at many criminal justice agencies. In contrast, cybersecurity minors (or majors) may be a competitive advantage for certain positions (digital forensics detective, for example) but would not be a competitive advantage for applicants seeking non-cyber focused positions.

Lastly, we believe it is important to acknowledge the role of COVID-19 in the results of this study. While many of the technologies already existed and were in use in the criminal justice sector, such as conferencing and meetings tools like Zoom and Microsoft Teams, methods of electronic payments

like Zelle and Venmo, messaging apps, and others, COVID pushed professionals to go all in, and deal with the potential consequences later. This includes the realm of information sharing, keeping records, communication with stakeholders and the community, among other areas of operation. Alexia demonstrated this in her example of using Venmo for billing patients, and the security and confidentiality risks associated with that as well as discussing the nuances of the legal and state licensing systems and practicing in a remote environment, which is applicable to helping professions and others in similar fields.

A. Limitations

This study was meant to be broad and exploratory in nature. While the small sample size does not make this study generalizable, it does offer perspectives from professionals in the field that encourage criminal justice faculty to consider the inclusion of cybercrime and cybersecurity within their programs. Our study was focused on understanding trends and new trajectories with cybercrime and cybersecurity that criminal justice agencies face that warrant future professionals to develop skills and knowledge in the area. Yet, we did not explore the applicability within specialized fields such as forensics.

Crime is increasingly becoming digital as individuals learn to adapt to the technologies available. As indicated by the participants in this study, equipping students in criminal justice with a basic understanding of cybercrime is also becoming increasingly important. Yet, the limitations of this study encourage subsequent research to further explore ways that skills, knowledge, and abilities can be included in degree programs to best prepare graduates for their future careers. Based on the findings and limitations from this study, we suggest three specific areas for future research. First, and most simply, more research is needed in this area. Future research can further explore the training needed in cybercrime and/or digital forensics for job placement. To do this, future research should emphasize larger samples and may want to include local, state, and federal agency perspectives. Additionally, future studies should include demographics to assess the prevalence of professionals with cyber knowledge in the criminal justice field and the diversity of the population with that skillset. Such information may be helpful in recruiting a diverse student population into criminal justice programs. Second, subsequent studies could extend this work by examining additional specialties within and related to criminal justice. For example, future research could explore if and how such knowledge of cybercrime will be beneficial to professionals working within forensics. Third, future research could explore the best practices for teaching cyber skills and knowledge to criminal justice students. In this emerging, interdisciplinary area, research on how to teach skills and specific pedagogical strategies will be beneficial. For example, do students learn best about prevention using games, scenarios, or applied learning experiences? More empirical pedagogical research in how to teach cyber skills and knowledge to the next generation of criminal justice professionals will be beneficial.

VI. CONCLUSION

This study focused on the broad and important role cybersecurity plays in the criminal justice system, along with the impact of cybersecurity skills, knowledge, and abilities that criminal justice graduates need upon graduation. Cybersecurity is more important than ever, and undergraduate institutions that provide criminal justice students with exposure to cybersecurity may offer their students a competitive advantage in the hiring process. This study also highlighted that higher education should focus on experiential learning to help students succeed upon graduation, and they must not forget about soft skills to include written and oral communication. Finally, interdisciplinary approaches in cybersecurity-related course offerings and programs are warranted.

REFERENCES

[1] Ackerman, R. (January 27,2019). Too few cybersecurity professionals is a gigantic problem for 2019. *TechCrunch*. Retrieved from: https://techcrunch.com/2019/01/27/too-few-cybersecurity-professionals-is-a-gigantic-problem-for-2019/

[2] Blazic, B.J. (2021). The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. *Technology in Society, 67(101769)*:1-13. https://doi.org/10.1016/j.techsoc.2021.101769

[3] Braun, V., & Clarke, V. (2012). Thematic analysis. In APA Handbook of research methods in psychology, Vol 2: Research designs: Quantitative, qualitative, neuropsychological, and biological (vol. 2, pp. 57–71). doi:10.1037/13620-004

[4] Byrne, J.M., & Marx, G.T. (2011). Technological Innovations in Crime Prevention and Policing. *A Review of the Research on Implementation and Impact*.

[5] Catota, F.E., Morgan, M.G., Sicker, D.C. (2019). Cybersecurity education in a developing nation: the Ecuadorian environment. *Journal of Cybersecurity,* 5(1),1-19. https://doi.org/10.1093/cybsec/tyz001

[6] Chowdhury, N., & Gkioulos, V. (2021). Key competencies for critical infrastructure cyber-security: a systematic literature review. *Information and Computer Security, 29*(5), 697-723. https://doi.org/10.1108/ICS-07-2020-0121

[7] Coss, C. (2016). Using financial intelligence to target online fraud victimization: Applying a tertiary prevention perspective. *Criminal Justice Studies, 29*(2), 125-142.

[8] Cremin, H., Sellman, E., & McCluskey, G. (2012). Interdisciplinary Perspectives on Restorative Justice: Developing Insights for Education. *British Journal of Educational Studies*, *60*(4), 421–437. https://doi.org/10.1080/00071005.2012.738290

[9] Dawson, J. & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology*. 9:744. doi: 10.3389/fpsyg.2018.00744

[10] El Messaoudi, M. (2021). Soft Skills: Connecting Classrooms with the Workplace--A Systematic Review. *Universitepark Bulletin*, *10*(2), 116–138. https://doi.org/10.22521/unibulletin.2021.102.2

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

[12] Griffiths, C. (2023, December 5). *The latest 2023 cyber crime statistics (updated May 2023).* AAG. https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=The%20growing%20cost%20of%20cyber%20crime&text=The%20average%20cost%20of%20a,to%20%2410.5%20trillion%

[13] Harkin, D., & Whelan, C.T. (2021). Perceptions of police training needs in cyber-crime. International Journal of Police Science & Management, 24, 66 - 76. DOI:10.1177/14613557211036565

[14] Hilton, M. (2008). Skills for Work in the 21st Century: What Does the Research Tell Us? *Academy of Management Perspectives*, 22(4), 63–78. https://doi.org/10.5465/AMP.2008.35590354

[15] Hitchcock A, Holmes R and Sundorph E (August, 2017) *Bobbies on the Net: A Police Workforce for the Digital Age*. London: Reform. Retrieved fromhttps://reform.uk/wpcontent/uploads/2018/10/Reform_Bobbies_on_the_net.pdf

[16] Holt, T. J. (2016). *Cybercrime Through an Interdisciplinary Lens*. Taylor & Francis Group.

[17] Hoffman, L. J., Burley, D., & Toregas, C. (2011). Thinking Across Stovepipes: Using a Holistic Development Strategy to Build the Cybersecurity Workforce. *IEEE Security and Privacy*, 1(13).

[18] Johnson, D., Faulkner, E., Meredith, G., & Wilson, T. J. (2020). Police functional adaptation to the digital or post digital age: Discussions with cybercrime experts. *The Journal of Criminal Law*, 84(5), 427-450. https://doi.org/10.1177/0022018320952559

[19] Koong, K.S. & Liu, L.C. (2002) A Study of the Demand for Information Technology Professionals in Selected Internet Job Portals. Journal of Information Systems Education 13(1) pp. 21-28. https://jise.org/Volume13/n1/JISEv13n1p21.pdf

[20] Lanier, M.M., & Cooper, A. T. (2016). From papyrus to cyber: How technology has directed law enforcement policy and practice. *Criminal JusticeStudies,29(2),92-104. https://doi.org/10.1080/1478601X.2016.1170280*

[21] Libicki, M.C., Senty, D., Pollak,J. (2014). *Hackers Wanted: An Examination of the Cybersecurity Labor Market.* RAND Corporation. http://www.jstor.org/stable/10.7249/j.ctt7zvzmj

[22] Mahibha, G., & Balasubramanian, P. (2020). A critical analysis of the significance of the eCourts information systems in Indian courts. *Legal InformationManagement*,20(1),47-53. https://doi.org/10.1017/S1472669620000092

[23] Miranda, D. (2020). Body-worn cameras 'on the move': exploring the contextual, technical and ethical challenges in policing practice. *Policing andSociety(32),*1,18-34.https://doi-org.libproxy.uccs.edu/10.1080/10439463.2021.1879074

[24] NIST (n.d). *Cybersecurity - glossary: CSRC*. CSRC Content Editor. Retrieved from https://csrc.nist.gov/glossary/term/cybersecurity

[25] Nodeland, B., Belshaw, S., & Saber, M. (2019). Teaching cybersecurity to criminal justice majors. *Journal of Criminal Justice Education, 30*(1), 71-90.

[26] Noll, C.L. & Wilkins, M. (2002) "Critical skills of IS professionals: a model for curriculum development." Journal of Information Technology Education 1(3): pp. 143-154.

[27] Nouh, M., Nurse, J. R., Webb, H., & Goldsmith, M. (2019). Cybercrime investigators are users too! Understanding the socio-technical challenges faced by law enforcement. *arXiv preprint arXiv:1902.06961. https://doi.org/10.48550/arXiv.1902.06961*

[28] Parrish, A., Impagliazzo, J., Raj, R.K., Santos, H., Asghar,M.R., Jøsang,A., Pereira, T., & Stavrou, E. (2018). Global perspectives on cybersecurity education for 2030: A case for a meta-discipline. In Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018 Companion). *Association for Computing Machinery,* New York, NY, USA, 36–54. https://doi.org/10.1145/3293881.3295778

[29] Payne, B.K. (2016). Editor's introduction: Special issue on cybersecurity and criminal justice. *Criminal Justice Studies, 2*9(2) 89-91.

[30] Payne, B. K., He,W.,Wang, C., Wittkower, D. E., & Wu,H.(2021). Cybersecurity, Technology, and Society: Developing an Interdisciplinary, Open, General Education Cybersecurity Course. *Journal of Information SystemsEducation*,*32*(2),134–149. https://aisel.aisnet.org/jise/vol32/iss2/6/

[31] Payne, B. K., & Hadzhidimova, L. (2018). Cyber security and criminal justice programs in the United States: Exploring the intersections. *International Journal of Criminal Justice Sciences, 13*(2).

[32] Pfefferkorn, R., (2020) 'Deepfakes' in the Courtroom. *Boston University Public Interest Law Journal*, Vol. 29, No. 2, 2020. https://ssrn.com/abstract=4321140

[33] Rios, J. A., Ling, G., Pugh, R., Becker, D., & Bacall, A. (2020). Identifying Critical 21st-Century Skills for Workplace Success: A Content Analysis of Job Advertisements. Educational Researcher, 49(2), 80-89. https://doi.org/10.3102/0013189X19890600

[34] Russo, J., Woods, D., Shaffer, J.S., & Jackson, B.A. (2019). Countering threats to correctional institutional safety: Identifying innovation needs to address current and emerging concerns. *RAND Corporation.* https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2933/RAND_RR2933.pdf

[35] Saunders, B., Sim, J., Kingstone, T., (2019). 'Saturation in Qualitative Research: exploring Its Conceptualization and Operationalization'. *Quality & Quantity* 52(4): 1893–1907

[36] Senjo, S. (2004). An analysis of computer related crime: Comparing police officer perceptions with empirical data. *Security Journal, 17*(2), 55-71.

[37] Statt, N. (2018, July 26). Idaho prison inmates exploited tablet vulnerability to steal $225,000 in credits. The Verge. https://www.theverge.com/2018/7/26/17619972/idaho-prison-inmates-tablet-hacks-jpay-stolen-credits-250-thousand

[38] Stewart, C., Wall, A., & Marciniec, S. (2016). Mixed Signals: Do College Graduates Have the Soft Skills That Employers Want? *Competition Forum*, *14*(2), 276–281.

[39] Succi, C., & Canovi, M. (2020). Soft skills to enhance graduate employability: Comparing students and employers' perceptions. *Studies inHigherEducation*,*45*(9),1834–1847. https://doi.org/10.1080/03075079.2019.1585420

[40] Surraka, S. (2005).Analysis of technical skills in job advertisements targeted at software developers. *Informatics in Education, 4*(1), 101-122.

[41] Sloan III, J. J., & Buchwalter, J. W. (2017). The State of Criminal Justice Bachelor's Degree Programs in the United States: Institutional, Departmental, and Curricula Features. *Journal of Criminal Justice Education*,*28*(3),307–334. https://doi.org/10.1080/10511253.2016.1240212

[42] Van Slyke, C. Clary, G., Ellis, S., & Maasberg, M. (2019). Employer preferences for cybersecurity skills among information systems graduates. *Association for Computing Machinery*, 131-134. https://doi-org.libproxy.uccs.edu/10.1145/3322385.3322418

[43] Wheatley, S. (2021, March 2). Charting new education pathways to fill the cybersecurity skills gap. *CSO.* Retrieved from *https://www.csoonline.com/article/3609524/charting-new-education-pathways-to-fill-the-cybersecurity-skillsgap.html#:~:text=The%202020%20Cybersecurity%20Workforce%20Study,forward%2C%20the%20gap%20remains%20significant.*

[44] Willits, D., & Nowacki, J. (2016). The use of specialized cybercrime policing units: An organizational analysis. *Criminal Justice Studies, 29*(2), 105-124. http://dx.doi.org/10.1080/1478601X.2016.1170282

[45] Winger, G., Ellis, S., & Glover, D. (2023). Bridging the Digital Gap: Teaching Cyber Strategy and Policy through a Crisis Simulation. *International Studies Perspectives,* https://doi.org/10.1093/isp/ekad001