Journal of Cybersecurity Education, Research and Practice

Volume 2022 | Number 1 Article 2

July 2022

Assessing the Practical Cybersecurity Skills Gained Through Criminal Justice Academic Programs to Benefit Security Operations Centers (SOCs)

Lucy Tsado
Lamar University, ltsado@lamar.edu

Jung Seob "Scott" Kim
Lamar University, jkim5@lamar.edu

Assessing the Practical Cybersecurity Skills Gained Through Criminal Justice Academic Programs to Benefit Security Operations Centers (SOCs)

Abstract

Private-sector and public-sector organizations have increasingly built specific business units for securing company assets, reputation, and lives, known as *security operations centers* (SOCs). Depending on the organization, these centers may also be referred to as global security operations centers, *cybersecurity* operations centers, fusion centers, and corporate command centers, among many other names. The concept of centralized function within an organization to improve an organization's security posture has attracted both the government and the private sectors to either build their own SOCs or hire third-party SOC companies.

In this article, the need for a multidisciplinary approach to cybersecurity education at colleges and universities, including in liberal arts programs, with criminal justice as an example of a liberal arts program was discussed. There is a need for academic institutions to incorporate certain policies to ensure that students in liberal arts are included in the cybersecurity career mix. Cybersecurity is a field that encompasses many skill sets, both technical and nontechnical. The practical cybersecurity skills gained through liberal arts programs do not align with the high demand for these skills in the field to benefit SOCs. Additionally, the skills gap in the industry is increasing, meaning there is room for students with nontechnical majors to join the cybersecurity field.

Liberal arts programs, specifically criminal justice programs, must be evaluated to align with the demand for skills in the government sector and the private sector; these programs must also help students apply the knowledge learned through criminal justice courses in real-world cases to benefit SOCs. We examine academic institutions in Texas as the basis for our discussion.

Keywords

Security operations center (SOC), cybersecurity skills, multidisciplinary approach, academic institutions, liberal arts programs, criminal justice programs, technical skills, nontechnical skills, cybersecurity, digital forensics

INTRODUCTION

The rise of cybercrime, data breaches, ransomware attacks, and zero-day vulnerabilities to insider threats increasingly dominates news media. The definition of cybercrime is complex because of the nature of cybercrime and technological advancement, but it can generally be described as the use of information and communications technology to commit a crime, such as illegally accessing, transmitting, or manipulating data.

Anyone with access to the internet can find a plethora of articles related to modern cybersecurity. The recent ransomware attacks on Kaseya, Colonial Pipeline, and SolarWinds, all of which had far-reaching effects on critical infrastructure and third-party vendors, are the most recent high-profile attacks. However, in recent months, unprecedented incidents of ransomware targeting private sector companies and government organizations have also occurred. Although high-profile attacks are widely circulated throughout the media, many attacks on smaller companies receive little or no media coverage. Moreover, companies are struggling to hire qualified candidates to defend their networks and critical infrastructure.

Problem: The Cybersecurity Skills Gap

Recently, the Director of the Federal Bureau of Investigation (FBI) Chris Wray compared the challenge in responding to the issue of unprecedented ransomware attacks in the United States to that of responding to the 9/11 terror attacks. He therefore states that the response to the recent spate of unprecedented cyberattacks should be similar to the swift and decisive response to the 9/11 terror attacks (Fung et al., 2021). Furthermore, the Department of Homeland Security (DHS) quoted the Cybersecurity and Infrastructure Security Agency (CISA) assistant director of cybersecurity in a press release, stating, "CISA sees the growing cybersecurity workforce shortage in the United States as a national security risk" (DHS, 2020, para. 3). The International Information System Security Certification Consortium $(ISC)^2$, an organization that conducts research on the cybersecurity field and its careers, stated in 2017 that the shortage of cybersecurity professionals is growing, and organizations should start looking for nontechnical skill sets ($(ISC)^2$, 2017). $(ISC)^2$ is also calling for other recruiting channels to involve people with other skill sets in the field ($(ISC)^2$, 2021a).

Why Is This Paper Important?

The government has made great strides, which are paramount in tackling the overall cybersecurity challenge facing the nation, in addressing cybersecurity education

and workforce issues. The government, through the National Institute of Standards and Technology (NIST), has structured the workforce using the NIST Cybersecurity Framework. The National Security Agency, along with the DHS, has cosponsored the Centers of Academic Excellence (CAE) designation to streamline cybersecurity education at institutions of higher education to meet the demand in the field. The establishment of organizations such as the National Initiative for Cybersecurity Education and the National Initiative for Cybersecurity Careers and Studies have also helped organize cybersecurity education and address workforce issues. However, these efforts are still largely deficient in engaging nontechnical majors in cybersecurity education.

Cybersecurity is a broad term. Within cybersecurity, there are many specialized fields, such as digital forensics and incident response, cyber threat intelligence, governance risk and compliance, insider threats, and information security assurance. Similarly, cybercrime is also a broad term; it can range from financial crime, identity fraud, social network fraud to unauthorized system access and the exchange of child pornography content on the deep-dark web. The aforementioned cybersecurity fields are practical areas or skill sets that criminal justice students can engage in. To fully defend against, respond to, and investigate cybercrimes and cybersecurity incidents, organizations are likely to hire individuals with technical skills, investigative skills, communication, and report-writing skills rather than those with general liberal arts research skills.

In this article, we intend to bridge the technical and nontechnical knowledge and skills gap in criminal justice academic programs by examining how these programs can be involved in cybersecurity education, training, and workforce issues, using the example of liberal arts programs in Texas.

The Solution to the Problem

Large, private-sector corporations usually have some type of SOC to provide physical and/or information technology security protection that operates 24/7 to detect threats. Although SOCs may vary from company to company, it is crucial for entry-level analysts to be able to work under pressure, document their processes, and produce timely reports. Cybersecurity education materials within criminal justice programs must expose students to these types of real-scenario environments so they can achieve hands-on experience and learn requisite skills for success in any type of SOC.

Individuals with technical skills can learn criminal concepts in cybercrime courses when given the opportunity; however, criminal justice students have challenges learning the technical components of cybersecurity if they lack the appropriate resources. Liberal arts programs do not typically include cybersecurity

courses in their curricula. Within the criminal justice field in particular, the lack of cybersecurity and digital forensics courses leads to inadequate preparation of students for real case experiences in responding to or defending against criminal behavior in cyberspace. The expansion of hands-on cybersecurity and digital forensics courses within criminal justice programs is highly desirable, and the courses taught must reflect employers' required skills and real case scenarios.

Although some required technical skills may be gained through internships, apprenticeships, and technical training, some cybersecurity positions require nontechnical skills as well, such as reviewing company or government policies, business continuity planning, risk analysis, effective communication with stakeholders, quick production of reports, organized process documentation writing, and briefing of various audiences.

Criminal justice degree programs should not only focus on careers in law enforcement agencies, courts, and corrections but also provide students with the knowledge and skills to pursue careers in any sector—government, private, academia, and nongovernmental organizations. According to a survey by the National Center for Education Statistics (NCES) about unemployment rates among individuals aged 25–29 with bachelor's degrees, criminal justice ranked among the top six fields of study with the highest rates, along with political science and other liberal arts majors (NCES, 2020). Moreover, graduates of criminal justice programs have one of the highest percentages of unemployment by degree program, at 73.2% (Redden, 2020).

If criminal justice programs can equip students with relevant skills, technical experiences, and cybersecurity and digital forensics training, these degrees will have higher values in the job market and give students the opportunity to be competitive candidates for jobs in cybersecurity. This would also expand students' professional career outlooks to include cybersecurity and digital forensics as potential career trajectories.

RESEARCH QUESTIONS

To research the skill requirements for criminal justice students to be competitive in SOCs, we asked the following questions:

A. What are the connections, if any, between cybersecurity and criminal justice in practical settings?
B. When schools offer cybersecurity courses, how many of these courses are included in criminal justice programs?
C. What are the technical skill requirements common among private companies and public organizations?

D. What are the nontechnical requirements common among private companies and public organizations?
E. How do we bridge the gap between the skills that are taught and those that are in demand?

What Are the Connections Between Cybersecurity and Criminal Justice in Practical Settings?

Criminal behavior in cyberspace requires a response; therefore, criminal justice students should be taught these skills. There is also a need to introduce the human factor in cybersecurity education—a skill that criminal justice students can bring to the table. Rege et al. (2019) demonstrated the human factor to be a valuable multidisciplinary concept. Their research involved computer science students and criminal justice students conducting a shoulder surfing experiment, and the research helped explain the importance of the human factor in social engineering, which is an important and emerging aspect of cybersecurity.

By virtue of their investigative nature, criminal justice majors are typically drawn to careers in law enforcement. The law enforcement career field often involves the duty of responding to crimes in cyberspace (Tsado & Osgood, 2022). Although the field of law enforcement is not directly connected to SOCs, it involves response to cybercrime, which falls within digital forensics, an integral part of SOCs. Therefore, digital forensics must become an integral part of criminal justice programs. Such topics as motivations and techniques, the adversary model (resources, capabilities, intent, motivation, risk aversion, access) and types of attacks (and the vulnerabilities that enable them), social engineering, insider problems, and legal issues, which are associated with cyber threats, are well suited to criminal justice students because they deal with the human factor (see the list of nontechnical knowledge units [KUs] included later). Therefore, it is in the interest of criminal justice academic departments to ensure their students learn how to not only respond to cybercrime and cyberattacks (digital forensics) but also prevent and mitigate cybercrime and cyberattacks. Focusing on these important KUs will help these students in the cybersecurity field, giving them a wider purview of career choices (including careers within SOCs).

The complete list of nontechnical KUs is available on the National IA Education and Training Programs (NIETP) website. The KUs referred here are found on page 21. This list includes required topics, some of which are typically taught in the cybercrime courses of many criminal justice programs. Following is a list of nontechnical KUs:

1. Motivations and techniques
2. The adversary model (resources, capabilities, intent, motivation, risk aversion, and access)
3. Types of attacks (and the vulnerabilities that enable them)
   a. Password guessing/cracking
   b. Backdoors/trojans/viruses/wireless attacks
   c. Sniffing/spoofing/session hijacking
   d. Denial of service (DOS)/distributed
   e. DOS/BOTs
   f. Media access control address spoofing/web application attacks/zero-day exploits
   g. Advanced persistent threat (APT)
4. Events that indicate an attack is/has happened
5. Attack timing (within *x* minutes of being attached to the net)
6. Attack surfaces/vectors and trees
7. Covert channels
8. Social engineering
9. The insider problem
10. Threat information sources (e.g., CERT)
11. Legal issues associated with cyber threats

We suggest that criminal justice academic departments create courses in cybercrimes, cybersecurity, and digital forensics. They could also create short-term certificate programs and teach these courses while encouraging students to acquire professional certifications in these fields.

When Schools Offer Cybersecurity Courses, How Many of These Courses Are in Criminal Justice Programs?

When academic institutions of higher learning offer cybersecurity courses, hardly any are housed in liberal arts programs such as criminal justice. While this is understandable, the assumption that cybersecurity is a technical field is not entirely true. Many of the requisite skill sets in some cybersecurity jobs are technical, but there are several others that are not (see the aforementioned list of nontechnical KUs). In fact, cybersecurity is a multidisciplinary field. For example, upon examination of some universities, some of their cybersecurity-related majors may be in computer science or information technology departments, but others are found in business and engineering (see Table 1). In our search using a study by Belshaw et al. (2020) and CAE-designated schools in Texas, we found that no cybersecurity majors or programs had any substantive presence in any liberal arts college or department.

According to Belshaw et al. (2020), the current academic institutions in Texas that offer cybersecurity courses as part of their bachelor's degree programs are as follows:

1. DeVry University (B.S. in Cybersecurity; College of Engineering)
2. LeTourneau University (B.S. in Computer Science: Cybersecurity)
3. Southern Methodist University (B.S. in Cybersecurity)
4. Sul Ross State University (B.S. Computer Science: Cybersecurity)
5. Texas A&M University–Corpus Christi (B.S. in Cybersecurity and Infrastructure; Department of Computing Science)
6. The University of Texas at San Antonio (B.B.A. in Cybersecurity; College of Business: Department of Information Systems and Cybersecurity)
7. University of the Incarnate Word (B.S. in Cybersecurity)
8. Wayland Baptist University (B.A.S. in Cybersecurity)

Although Belshaw et al. (2020) missed several schools—especially those designated as CAE institutions—an examination of CAE-designated schools revealed that cybersecurity did not have a strong presence in liberal arts programs at any schools. See Table 1:

S/Number	**CAE-Designated Universities and Colleges in Texas**	**Type of Degree**	**Department Housing Cybersecurity-Related Programs**
1	El Paso Community College	Associate	Cybersecurity Center
2	Hill College	Associate	Cybersecurity Center
3	Houston Community College	Associate	Science, Technology, Engineering, and Mathematics
4	Laredo College	Associate	Center for Cyber Education: Computer Technology Department
5	McLennan Community College	Associate	Computer and Information Technology
6	Our Lady of the Lake University	Bachelor, Certificate Program	Center for Cyber Leadership; School of Business
7	Sam Houston State University	Bachelor	Science and Engineering Technology
8	San Antonio College	Associate	Communication, Design, CIS, Music Business, and RTB
9	South Texas College	Associate	Division of Math, Science, IT and Bachelor Programs
10	Southern Methodist University	Master	School of Engineering
11	St. Philip's College	Associate	Science and Technology

12	Texas A&M– San Antonio	Bachelor	Department of Computing and Cyber Security; College of Business
13	Texas A&M University	Bachelor, Master, Certificate Programs	Texas A&M Cybersecurity Center
14	Texas A&M University	Bachelor, Master, Certificate Programs	Texas A&M Cybersecurity Center
15	Texas A&M University–Corpus Christi	Upcoming	College of Science & Engineering
16	Texas State Technical College – Harlingen Campus	Associate	Computer & Information Technology
17	The University of Texas at Austin	Concentration	Computer Science
18	University of Dallas	Master	College of Business
19	University of Houston	Master	College of Technology
20	University of North Texas	Bachelor, Master, Certificate Programs	Computer Science and Engineering
21	University of Texas at Dallas	Master	School of Economic, Political and Policy Sciences; School of Engineering and Computer Science
22	University of Texas at El Paso	Certificate	College of Engineering: Department of Computer Science
23	University of Texas at San Antonio	Bachelor, Master, Master Certificate Program	College of Business

Table 1: CAE-Designated Schools in Texas and Their Cybersecurity-Related Programs

It is obvious that criminal justice students cannot be competitive candidates for SOC jobs if they are not learning the related skills or even being considered as prospective cybersecurity professionals—even as the industry is calling out for such changes. We believe the best approach may be not to house cybersecurity in any one academic department but rather to take a multidisciplinary approach. It makes sense to have a cybersecurity center in place to handle all issues related to cybersecurity awareness, training, and curricula. This suggestion seems to have been implemented by a few departments in the Texas schools sampled in Table 1. A multidisciplinary approach will most likely require that schools use a top-down approach to manage all cybersecurity issues, including curricula. Tsado (2019) stated that it makes sense for cybersecurity education at a school to have a top-down, multidisciplinary approach to ensure all academic departments in a school are involved in cybersecurity education. This approach also allows institutions of higher learning to use their resources judiciously and collectively rather than follow

a piecemeal approach; a piecemeal approach results in several departments of an institution approaching cybersecurity education and related matters from different perspectives. In contrast, a multidisciplinary approach ensures not only conservative use of resources (among other advantages) but also that all academic departments, rather than only technical departments, have the opportunity to educate students in cybersecurity.

What Are the Technical Requirements That Private-Sector Companies Require in Security Operations Centers (SOC)?

Before discussing technical requirements, it is important to understand the functionalities, capabilities, and missions of SOCs. Generally, a SOC will have the core function of serving as an intelligence hub that gathers data in real time from the organization's networks, servers, and other digital assets, using automated intelligence to identify, prioritize, and respond to potential information security threats (CrowdStrike, 2021). Below is an image of a process workflow diagram for security incident management (Taurins, 2020).

Figure 1: How to Set Up CSIR and SOC

Companies require hands-on experience in network security, basic computer skills, and coding/programming knowledge. However, current course offerings vary greatly among academic institutions, and technical skills vary greatly among private-sector corporations. To address these differences, we explored the current technical skills requirements of some companies in Texas by taking a sample of job advertisements from May 1, 2021, to May 31, 2021. The assessment provided here focuses on full-time entry-level jobs in Greater Houston, Texas. We used LinkedIn and Indeed, two primary job search tools, to identify cybersecurity jobs in SOCs. Our search was collated, and it yielded the information displayed in Table 2.

Position	**Job Description**	**Knowledge, Skills, and Abilities**
Cybersecurity analyst	1. Analyze network traffic to identify anomalous activity and potential threats to network resources 2. Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack 3. Receive and analyze network traffic alerts from various sources within the enterprise and determine possible causes of such alerts 4. Provide timely detection, identification, and alerting of possible attacks and distinguish these incidents and events from benign activities	1. Basic knowledge and experience with one or more IT security technologies, including firewalls, IPS, SIEM, DLP, network/host protection, application security, and data protection 2. Understanding of TCP/IP networking 3. Experience in security monitoring, intelligence gathering, and intelligence analysis using log management tools such as Splunk, ArcSight, QRadar, and Nitro 4. Familiarity with security best practices and industry standards (e.g., NIST)
Threat intelligence analyst	1. Provide subject-matter expertise to the development of specific indicators of cyber operations 2. Identify threat tactics and methodologies 3. Monitor open-source websites for hostile content directed toward organizational or partner interests 4. Provide timely notice of imminent or hostile intentions or activities that may impact organization objects, resources, or capabilities	1. Experience with host- and network-based protection 2. Experience in analyzing security vulnerabilities, various exploitation techniques, and malware behaviors 3. Knowledge of TCP/IP and other networking and industrial protocols 4. Experience writing network and endpoint signature detections using SNORT and YARA 5. Hands-on experience with structured analytical techniques, the intelligence cycle, threat intelligence assessments, and intelligence writing methodologies

Digital forensics analyst	1. Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator of a network intrusion or other crime 2. Perform real-time forensics analysis, file signature analysis, and real-time cyber defense incident tasks 3. Perform Tiers 1, 2, and 3 malware analysis and dynamic analysis to boot an image of a drive to view intrusions as the user may have seen them 4. Capture and analyze network traffic associated with malicious activities using network monitoring tools	1. Experience in analyzing network traffic, firewall logs, and host-based security appliance logs 2. Experience in performing forensics analysis on popular operating systems 3. Experience with forensics tools such as EnCase, Forensics ToolKit, and Cellebrite 4. Understanding and practical knowledge of operating system design, computer networking, network protocols, and computer file systems

Table 2: Select Cybersecurity and Digital Forensics Positions, Job Descriptions, and Required Skill Sets

What are the Nontechnical Requirements Common Among Private Companies and Public Organizations?

Find below some nontechnical requirements required for successful entrants to SOC positions.

The Human Factor

There is no doubt that technical skills are needed in cybersecurity; however, there is a human factor to cybersecurity that cannot be ignored. An example of the human factor is seen in social reconnaissance, in which a criminal gathers information about a target to find vulnerabilities. Many technical-oriented students have not been taught about this and are unaware of how to build systems and provide security with the human factor in mind (Rege et al., 2019). Understanding human behavior is part of criminology (the study of the causes of crime), criminal justice (the study of responses to criminal behavior), and other liberal arts majors, such as psychology. Therefore, these are skills that criminal justice and other liberal arts majors can bring to the table in both prevention of and response to criminal behavior involving cyberspace. As stated by $(ISC)^2$, (2017), gone are the days when cybersecurity could be addressed by only those with technical skills.

Creating teams of students in courses, some with technical and others with human behavioral skill sets provides an advantage in fighting cybercrime and cyber threats. Understanding the motives behind criminal behavior is an advantage that criminal justice majors can bring to the table.

Critical Thinking Skills

Critical thinking is a foundational skill for cybersecurity professionals (Austin, 2019; $(ISC)^2$, 2021b). The ability to ask why and how is very important in solving today's challenges in cybersecurity. Therefore, students must be able to develop these skills while they are still in school. With the recent increase of disinformation and misinformation in the media, it is easy to become sidetracked by false narratives or misleading information. Students must be able to distinguish between biased points and objective facts. The FBI intelligence analyst's critical thinking requirements include the following (FBI.gov):

- Gather and analyze information and draw well-reasoned conclusions;
- Use a logical and systematic approach to analyze data, problems, and situations;
- Differentiate between relevant and irrelevant information;
- Discern relevant merits and deficiencies in logic and evaluate the credibility of information; and
- Integrate diverse information to detect relationships, patterns, and trends.

Again, these are not technical skills but rather critical thinking skills. Criminal justice courses may integrate an exam that tests students' abilities to respond to real-world security cases and produce timely reports. Because the exam would reflect a real-world situation, there would be an abundant amount of data; the ability to analyze large amount of information would be assessed during the exam, thus bolstering critical thinking skills.

Communication

Security analysts communicate with a variety of audiences, including vendors, customers, clients, coworkers, managers, human resources staff, legal professionals, and many others. Communicating technical issues to technical and nontechnical audiences is a critical ability, reflected in the high position of communication skills on the list of skills required for security information analysts (Dice.com, n.d.; $(ISC)^2$, (2021a); $(ISC)^2$, (2021b)). Practicing a bottom-line upfront (BLUF) method is highly desirable when communicating with leaders; BLUF is a policy writing style used in informal military correspondence to cover main points so the respondents can absorb the main points of a message without reading the entire message.

Most companies communicate through email. Testing communication skills through emails can be an effective way to communicate with different teams. Criminal justice programs must integrate communication of information security language into their curricula.

Creativity, Hands-On Learning, and Real-Life Scenarios

To reiterate, academic institutions must encourage students to participate in real-world settings or hands-on experiential learning. Hands on learning is a great tool for teaching students cybersecurity concepts (Konak, 2018). Most criminal justice programs require an internship as a course. In addition to internships, criminal justice programs and professors can encourage and sponsor student participation in cybersecurity competitions, hackathons, and conferences beyond what is available on campus. Academic institutions must be active online communities, going beyond physical campuses, to conduct multidisciplinary cybersecurity research, education, and innovation. Although winning competitions may bring prestige to a program, the purpose of competitions is for students to actively communicate with their peers and learn how others approach cybersecurity problems. These exchange hubs will facilitate the exchange of creativity and mutual benefits among universities.

Research and Analysis

Security analysts perform in-depth investigations of networks and malware. Although many institutions require students to take criminal justice research classes, the reports that academic institutions produce are different than those produced by companies in the government and private sectors; this means that the collection methodology and process can vary as well. Analysts must collect data from both open sources and closed sources, and it is critical for students to learn where to gather data from, what types of data to gather, and how to build effective processes to collect relevant information. For information to turn into intelligence, a security analyst must be able to analyze the information. One way for criminal justice programs to expand these research and analysis skills is to integrate Sherman Kent's book, *Profession of Intelligence Analysis*, as part of the class's reading materials. Additionally, documenting the processes of gathering and analyzing data and information is extremely important.

Writing Skills

Security analysts produce a variety of reports, including tactical, operational, and strategic reports, for stakeholders. Cybersecurity analysts are required to write reports detailing how they performed their tasks so that others can understand (Day, n.d.). SANS, a security certification organization, has a course on writing

buttressing the importance of writing (SANS.org). Criminal justice courses must continue to require students to write such a variety of reports. Some classes require students to write essays during exams, which is an ideal way to practice producing a report in a short period of time. However, college courses must shift toward producing reports geared toward a variety of customers. In fact, courses should allow students to use the internet and other open-source intelligence sources to write their reports; not allowing students to use these sources only reinforces a tendency to regurgitate the information they learn in class, thus failing to support the skills of creativity, research, data collection, and intelligence analysis.

Documentation

Just as in writing, the importance of documentation is critical in the information security field (Day, n.d.). Every company will go through an audit or legal procedure at some point. In cybersecurity, documentation is important because it allows analysts to document what happens during a breach and why and how the breach is happening during the processes of threat analysis and response. The documentation process is vital in not only ensuring that these processes are documented but also aiding future prevention of attacks and repetition of successful approaches for future situations.

What Does Criminal Justice Bring to the Table? What Skills Do Criminal Justice Students Have That They Can Leverage?

Criminal justice is a field known to produce individuals who are theoretical in thinking; in other words, they consider why crime happens as well as how to prevent it from happening. This way of thinking can be an asset in the field of cybersecurity. Additionally, many facets of cybercrime are crimes of opportunity that happen based on human behavior and the modification thereof. Third, as stated earlier, many areas of cybersecurity are not technical in nature (as seen from the CAE KUs in Figure 1). The ability to gather and analyze information, write reports, and be creative are all skills that criminal justice students can learn in addition to other critical thinking skills to compete for jobs in the cybersecurity field.

The technical and nontechnical KUs are clearly mapped out by the NIST through the National Information Assurance Education and Training Programs (NIETP; see Figure 2). Criminal justice academic departments can develop academic programs based on nontechnical KUs in cybersecurity; they can also expand their students' skill sets by collaborating with other departments, such as computer science and engineering departments, in cross-training of students and introducing cybersecurity certification programs. One important move is to expose students to acquiring certifications in specific areas of cybersecurity that will make them competitive in their job searches before they graduate.

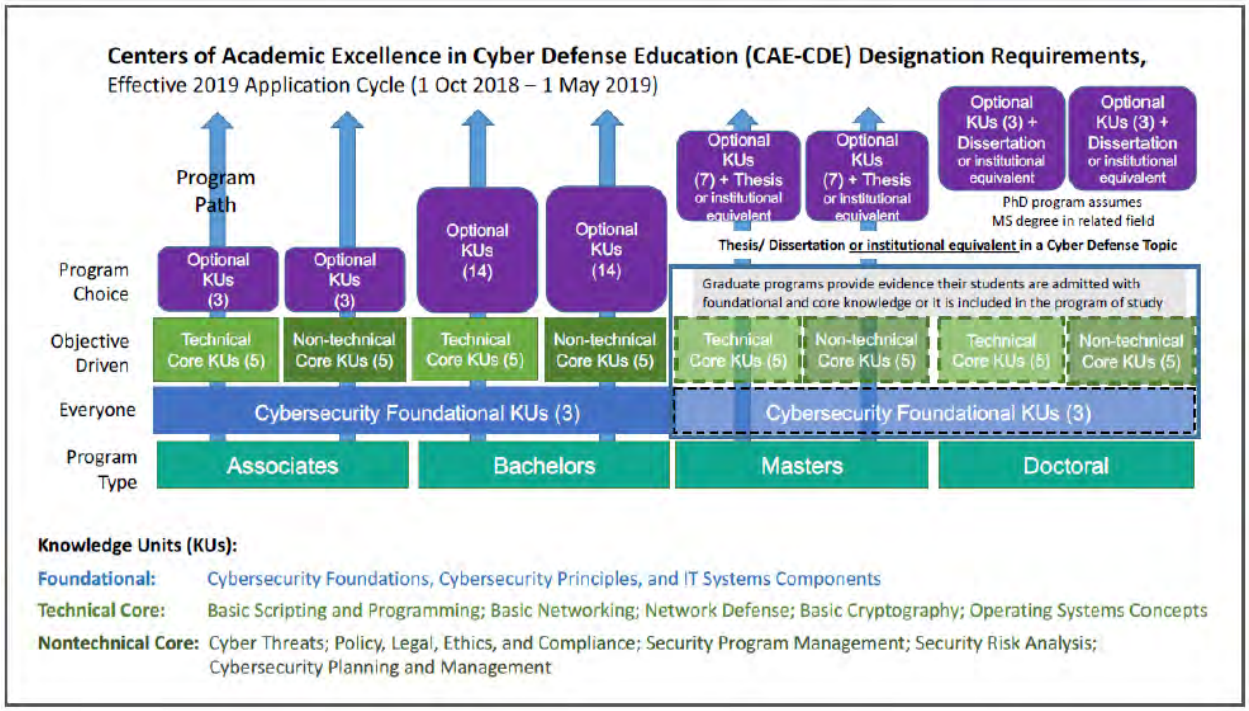

Figure 2: Technical and Nontechnical KUs for CAE Designations (available at https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2020_Knowledge_Units.pdf)

How Do We Bridge the Gap Between What Is Taught and What Is Needed?

We can bridge this gap in several ways: The first is by introducing courses or certificate courses in criminal justice academic programs that expose students to experiential, hands-on learning. Such courses must have labs embedded with hands-on learning scenarios. Additionally, criminal justice students should be afforded the opportunity of acquiring introductory, or short, certificate programs in specialty areas of cybersecurity and digital forensics, in which they can receive additional training and develop knowledge and skills required for entry-level jobs in the field.

Secondly, criminal justice academic programs should at a minimum, teach courses in cybersecurity and digital forensics and ensure that students have the opportunity to acquire cybersecurity and/or digital forensics entry-level introductory professional certifications, such as CompTIA Security+ and CompTIA Network, before graduation. Many cybersecurity and digital forensics

certification vendors are vendor-specific, meaning certifications are provided by the company that developed the software. Examples of such certifications include Forensic ToolKit and Access Data. As a guide, the CyberSeek tool can be used to determine which certifications are necessary for a specific job (see Table 3).

Entry-Level Role	Common Job Title	Top Required Skills	Top Requested Certifications
Cybersecurity specialist	1. Information security specialist 2. IT security specialist 3. IT specialist in information security 4. Information technology specialist in information security	1. Information security 2. Information systems 3. Information assurance 4. Network security 5. Security operations 6. Vulnerability assessment 7. Project management 8. Linux 9. NIST cybersecurity framework	1. SANS/GIAC Certification (Various) 2. CompTIA Security+ 3. Information Systems Certification 4. IT Infrastructure Library (ITIL) Certification
Cybercrime analyst	1. Digital forensics analyst 2. Cyber forensic specialist 3. Cybersecurity forensic analyst 4. Computer forensics analyst	1. Computer forensics 2. Linux 3. Information security 4. Consumer electronics 5. Hard drives 6. Information systems 7. Forensic toolkit 8. UNIX 9. Malware engineering	1. EnCase Certified Examiner (EnCE) 2. GIAC Certified Forensic Analyst 3. GIAC Certified Incident Handler (GCIH) 4. Certified Information Privacy Professional (CIPP)

Incident and intrusion analyst	1. Senior analyst, information security 2. Disaster recovery specialist 3. Network technical specialist 4. Audit project manager—information security	1. Information security 2. Project management 3. Information systems 4. Linux 5. Network security 6. Technical support 7. Intrusion detection 8. UNIX 9. Security operations	1. GCIH 2. CompTIA Security+ 3. ITIL Certification
IT auditor (possibly mid-level)	1. Senior IT auditor 2. IT audit consultant 3. IT audit manager 4. IT internal auditor	1. Internal auditing 2. Audit planning 3. Information systems 4. Sarbanes-Oxley 5. Accounting 6. Risk assessment 7. Information security 8. COBIT 9. Business process	1. Certified Information Systems Auditor (CISA) 2. Information Systems Certification 3. CompTIA Security+ 4. ITIL Certification

Table 3: List of Entry-Level Cybersecurity Roles and Their Required Certifications (adapted from Cyberseek.org; (available at https://www.cyberseek.org/pathway.html)

Thirdly, criminal justice programs must begin to look at other programs outside of criminal justice to inform curriculum development. For example, a cybersecurity certificate program of cybersecurity/and or digital forensics in criminal justice can include courses such as:

1. Introduction to Cybersecurity
2. Cybercrime
3. Operating Systems
4. Digital Forensics
5. Network Security
6. Vulnerability Assessment
7. Cybersecurity Risk and Business Continuity
8. Cybersecurity Governance and Leadership
9. Cybersecurity Law and Policy and Ethics

While some of these courses cover criminal justice knowledge of cybersecurity such as cybercrime, cybersecurity law and policy and cybersecurity risk, governance, and ethics, others like digital forensics, vulnerability assessment, operating systems and network security will give students hands-on experiential learning.

Lastly, a criminal justice department could also encourage students to take a different route by introducing an interdisciplinary minor in cybersecurity and digital forensic. The minor should be designed to allow students take fifteen to eighteen credit hours of the above listed courses depending on the track of interest to the students. Courses like network security and operating systems can be taken from other departments like computer science and engineering rather than criminal justice creating its own courses in these areas. Criminal justice degree programs should also focus on collaborating with other degree programs, such as computer science, international relations, business, accounting, engineering, and law, to address different types of crimes that criminal justice major students may face in their future careers.

To incorporate these cybersecurity education features into existing and new cybersecurity programs, top technical researchers, industry practitioners, and government leaders must be involved as authorities on cybersecurity curriculum to prepare students for adopting new trends and directions (Schneider, 2013). The cybersecurity programs' curriculum must include learning about the real-life cyber breaches with subtopics. Using real case studies will link individual security topics to real-world situations (Cai, 2018). In addition to these suggestions, criminal justice programs should require students to participate in workshops, conferences, and competitions.

CONCLUSION AND RECOMMENDATIONS

In this paper we emphasized the KUs required to successfully work as a SOC analyst. In institutions of higher learning, all criminal justice programs should have a cybersecurity track that requires students to take courses in network security, vulnerability assessment, digital forensics, ethics and compliance, data analysis, and so on. Aside from cybercrime courses, financial crime analysis and threat assessments expand the practical skills that students can utilize upon graduation. For example, money laundering is a prevalent financial crime, and criminal justice programs should require students to take courses that teach them financial literacy in addition to those that teach them how to investigate financial crimes and cybercrimes.

Furthermore, universities and colleges should provide a multidisciplinary environment centered on cybersecurity, in which technical and nontechnical students can learn from each other by taking courses together. In such an environment, students from all academic fields, including liberal arts programs, could benefit from career opportunities in cybersecurity. Therefore, schools will need to create multidisciplinary cybersecurity centers, or hubs, that address not only curricula but also career advancement and other activities that will generate interest in cybersecurity. Educational institutions must also drive robust academic programs that will provide nurturing environments for the continuous growth of cybersecurity-related activities (both academic and otherwise) not only within the schools but also in the surrounding communities. This will ensure that a cybersecurity ecosystem is built to involve both the school and the surrounding community, in which employers will engage in providing employment, internships, and apprenticeships to students from all academic fields (Tsado, 2019).

In conclusion, we suggest the following:

1. At the institutional level, cybersecurity curricula should be treated as an institution-wide issue. A top-down multidisciplinary approach is necessary.
2. Criminal justice programs can leverage and provide students with required KUs through rigorous coursework and certification courses that address deficiencies using hands-on learning curricula, internships, and apprenticeships.
3. Criminal justice programs should offer digital forensics specifically as a career alternative and include aspects of cybersecurity to give their students a competitive edge in the workforce, using the CAE KUs (as detailed by the NIETP) as a guide.
4. Criminal justice programs should provide opportunity and incentives for students to acquire cybersecurity and digital forensics certifications before they graduate.

5. Criminal justice programs should expose students to real-world experiential learning within courses, using labs, to provide them with hands-on experience or simulations of real-world cybersecurity issues.
6. Critical thinking skills should be built into criminal justice cybersecurity and digital forensics courses by using project-based curricula in which students can brainstorm and create solutions to problems; creativity should be encouraged in these courses. Research and analysis should be integral parts of all courses as well.
7. Criminal justice courses should also include communication, writing, and documentation training in all cybersecurity and digital forensics courses—especially courses that are project-based. Documentation and report writing should be integral parts of all courses in digital forensics and cybersecurity.

REFERENCES

Austin, N. (2019, October 7). *Fake news in cybersecurity education: Why critical thinking skills matter*. LinkedIn. https://www.linkedin.com/pulse/fake-news-cybersecurity-education-why-critical-thinking-nancy-austin

Belshaw, S., Nodeland, B., Underwood, L., & Colaiuta, A. (2020). Teaching about the dark web in criminal justice or related programs at the community college and university levels. *Journal of Cybersecurity Education, Research and Practice*, Vol. 2019: No. 2, Article 5. https://digitalcommons.kennesaw.edu/jcerp/vol2019/iss2/5?utm_source=digitalcommons.kennesaw.edu%2Fjcerp%2Fvol2019%2Fiss2%2F5&utm_medium=PDF&utm_campaign=PDFCoverPages

Cai, Y. (2018). Using Case Studies to Teach Cybersecurity Courses," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2018: No. 2, Article 3.

CrowdStrike. (2021, April 28). *Security operations center (SOC)*. https://www.crowdstrike.com/cybersecurity-101/security-operations-center-soc/

Davis, J. (n.d.). Sherman Kent and the profession of intelligence analysis. *The Sherman Kent Center for Intelligence Analysis. Occasional Papers: Volume 1, Number 5, Nov. '02* https://www.cia.gov/static/aa47b490ac1c52c04c467a248c5cbace/Kent-Profession-Intel-Analysis.pdf

Day, M. (n.d). *7 must-have skills for cybersecurity success*. https://startacybercareer.com/six-skills-needed-for-success-in-cyber-security/

Department of Homeland Security. (2020, October 30). *News release: DHS awards $2M to University of Illinois-led consortium to create national network of cybersecurity institutes.* https://www.dhs.gov/science-and-technology/news/2020/10/30/news-release-dhs-awards-2m-create-national-cybersecurity-network

Dice. Com. (n.d.). *Six skills you need to succeed in cybersecurity*. https://insights.dice.com/cybersecurity-skills/

Federal Bureau of Investigation (2021). *Intelligence analyst selection process: Candidate information*. https://www.fbijobs.gov/sites/default/files/intelligence_analyst_candidate_information_packet.pdf

Fung, B., Sands, G., Janfaza, R., & Cohen, Z. (2021, June 4). *FBI director sees "parallels"*

between challenge posed by ransomware attacks and 9/11. CNN. https://www.cnn.com/2021/06/04/politics/christopher-wray-cyberattacks-9-11/index.html

International Information System Security Certification Consortium (ISC)^2. (2017, June 7). *Global cybersecurity workforce shortage to reach 1.8 million as threats loom larger and stakes rise higher.* (ISC)^2 News. https://www.isc2.org/~/link.aspx?_id=3AD9CB67B85D4768B27E1D62FFA7D3A2&_z=z

International Information System Security Certification Consortium (ISC)^2. (2021a). *The cybersecurity career pursuers study: Build resilient cybersecurity teams*. https://www.isc2.org/-/media/ISC2/Research/2021/CybersecurityCareerPursuers-Study

International Information System Security Certification Consortium (ISC)^2. (2021b). *A Resilient cybersecurity profession charts the path forward*. (ISC)^2 Cybersecurity Workforce Study, 2021. https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

Konak, A. (2018). Experiential learning builds cybersecurity self-efficacy in K-12 students. *Journal of Cybersecurity Education, Research and Practice*, Vol. 2018: No. 1, Article 6.

National Center for Education Statistics. (2020). *Employment outcomes of bachelor's degree holders* [White paper]. The Condition of Education 2020. https://nces.ed.gov/programs/coe/pdf/coe_sbc.pdf

National IA and Education Training Program. (n.d.). NCAE Requirements and Resources-Knowledge Units. https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2020_Knowledge_Units.pdf

Redden, E. (2020, February 18). *41% of recent grads work in jobs not requiring a degree*. Inside Higher Ed. https://www.insidehighered.com/quicktakes/2020/02/18/41-recent-grads-work-jobs-not-requiring-degree

Rege, A., Mendlein, A., & Williams, K. (2019). Security and privacy education for STEM undergraduates: A shoulder surfing course project. *2019 IEEE Frontiers in Education Conference (FIE)*, 1–7. https://doi.org/10.1109/FIE43999.2019.9028560

SANS.Org. (n.d.). *SEC402: Cybersecurity writing: Hack the reader.* https://www.sans.org/cyber-security-courses/cyber-security-writing-hack-the-reader/

Schneider, F. B. (2013). Cybersecurity education in universities. *IEEE Security Privacy, 11(4),* 3-4. doi:10.1109/MSP.2013.84

Taurins, E. (2020, December 10). *How to set up CSIRT and SOC*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

Tsado, L. (2019) Cybersecurity education: The need for a top-driven, multidisciplinary, school-wide approach. *Journal of Cybersecurity Education, Research and Practice*, Vol. 2019: No. 1, Article 4. https://digitalcommons.kennesaw.edu/jcerp/vol2019/iss1/4

Tsado, L., & Osgood, R. (2022, forthcoming). *Careers in cybersecurity and digital forensics.* Rowman and Littlefield.