Building a Cybersecurity and AI Integrated Learning Pathway for Criminal Justice Professionals

Yan Bai
School of Engineering and Technology
University of Washington Tacoma
Tacoma, WA, USA
yanb@uw.edu
0000-0001-6260-9821

Juan Li
Department of Computer Science
North Dakota State University
Fargo, ND, USA
j.li@ndsu.edu
0000-0002-7668-5996

Abstract—With support from the National Science Foundation, The University of Washington Tacoma and North Dakota State University have developed scenario-based security curriculum and online showcase labs with interactive simulations and case studies across three progressive courses, revolutionizing cybersecurity education for Criminal Justice (CJ) professionals. By incorporating artificial intelligence into the curriculum, this project enhances CJ professionals' capabilities. Our goal is to develop a skilled workforce of CJ professionals with cybersecurity and privacy knowledge, addressing the critical need for such cybersecurity expertise in CJ. Literature review, focus group survey results, course framework tailored for CJ professionals, example course modules, and implementation results are presented.

Keywords—*Cybersecurity, Criminal Justice, Artificial Intelligence*

I. INTRODUCTION

A diverse and interdisciplinary cybersecurity workforce plays a crucial role in enhancing cybersecurity worldwide [1, 2]. Criminal justice (CJ) professionals are at the forefront of investigating cybercrimes and bringing cybercriminals to justice. Their expertise and efforts in cybersecurity are essential to maintaining the integrity of our digital ecosystem and ensuring the safety and security of individuals, organizations, and society. However, many CJ professionals have not received comprehensive cybersecurity education and training [5]. While cybercrime scholars have established themselves in academic organizations in criminology and criminal justice, and some graduate programs have been developed [6], many academic criminal justice and criminology programs lack dedicated courses on the topic. Moreover, many frontline criminal justice professionals lack the necessary training to effectively investigate and address cybercrimes [7], and frontline justice professionals are often unclear about the role they ought to play in responding to cybercrime and may be hesitant to engage in cybercrime professional training [8]. This knowledge gap poses significant challenges and limitations for effectively combating cybercrime [9,10].

We aim to bridge the cybersecurity education gap for CJ professionals. We conduct literature reviews and online focus group surveys about current cybersecurity education and trainings in criminal justice and identify key areas and cybersecurity topics within both criminal justice academia and practice. Based on our results, we create a tailored curriculum. During this process, we foster strategic partnerships between academia and CJ practitioners.

Section II summarizes qualitative data collected from criminal justice educators and practitioners regarding present cybersecurity education and trainings. Section III describes a progressive learning pathway for cybersecurity upskilling for CJ professionals. Section IV provides some examples of teaching modules. Section V concludes the paper and suggests future works.

II. BACKGROUND WORK

The literature reviews we conducted have indicated that 1) there is a strong need for effective training of law enforcement officers on dealing with ever-increasing cybercrimes [5]. Interactive training along with real-life examples in the areas of emerging digital technologies and up-to-date digital forensics are particularly demanding. Research has also shown that game-based training methods were popular [24]; 2) Less than one-fifth of CJ academic programs offer cybersecurity coursework in their CJ curricular [21]. Part of the future work about expanding cybersecurity in CJ education is educating CJ faculty about the interdisciplinary nature of cybersecurity, and motivating them to work with cybersecurity experts to embrace cybersecurity in many more CJ programs; and 3) Artificial Intelligence (AI) are being widely used in anomaly detection, threat identification, and automated incident response [22]. It necessitates the integration of AI into the cybersecurity curricula in all disciplines, including CJ programs [23]. To the best of our knowledge, few cybersecurity coursework in CJ curricula include AI components.

This research was, in part, supported by the National Science Foundation.

To further understand the current situation and needs for specific cybersecurity knowledge and skillsets in CJ fields, we have developed and conducted two online questionnaire surveys to CJ educators and practitioners. In reviewing the survey results, from twenty-two CJ instructors from public and private universities where bachelor's and master's CJ degrees are offered including four research-oriented institutions and four teaching-oriented institutions, we discovered that only 14% of CJ programs offer cybersecurity courses despite more than 76% of CJ educators believing it is important or very important to offer cybersecurity courses in CJ programs. The cybersecurity topics that CJ professors are interested in are broad ranging from social network security, privacy, digital forensics, computer network security, to legal and ethical issues. Moreover, over 76% of CJ educators are interested in participating in cybersecurity trainings.

Eighteen CJ practitioners have completed the online questionnaire surveys. Like the CJ educators who have taken the survey, they are well aware of the importance of cybersecurity education and trainings in CJ field. However, more than 82% are not quite familiar with cybersecurity. They indicated interest in learning cybersecurity topics related to their CJ careers, mainly in ethical hacking, privacy, digital investigation Internet security, and legal aspects of cyber investigation. Over 66% of CJ practitioners are interested in participating in cybersecurity trainings.

After analyzing the survey results, we have also identified the following problems in Cybersecurity education and training for CJ professionals.

1. The cybersecurity education and training content for CJ students and professionals is not closely related to CJ fields, hindering CJ professionals' ability to quickly transfer cybersecurity knowledge into practice, i.e., handling professional problems in real world, which aligns with findings from the literature.
2. Shortage of instructors who are experts in both CJ and cybersecurity and difficulties in assembling a multidisciplinary instructional team.

III. A PROGRESSIVE LEARNING PATHWAY

To address the issues of cybersecurity education in CJ described in Section II, we have worked with CJ professionals and advisory teams to develop the need-based curriculum tailed to CJ professional background and career requirements.

In order to achieve the above educational objectives, a progressive learning pathway is designed as three courses as shown in Figure 1.

Each course builds upon the knowledge and skills acquired in the previous courses, providing a structured and comprehensive learning experience. The progressive nature of the pathway allows CJ professionals to develop a solid foundation in cybersecurity and privacy through the introductory course. Subsequently, they can advance to specialized courses focusing on cyber forensics, cyber intelligence, and solving CJ-specific cyber challenges. This progressive learning pathway ensures a step-by-step acquisition of knowledge and skills, helping CJ professionals to become proficient in addressing cybersecurity challenges within the criminal justice domain. More notably, we integrate artificial intelligence (AI) into our courses to prepare CJ professionals to deal with emerging technological challenges in cybercrime investigations.

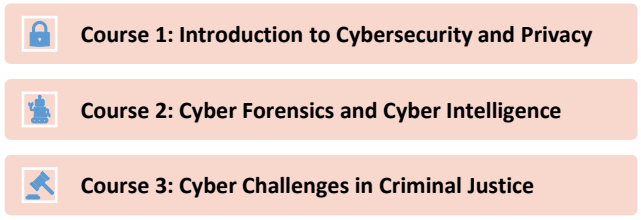


Fig. 1. A progressive learning pathway.

Course 1, Introduction to Cybersecurity and Privacy, provides CJ professionals with basic knowledge in cybersecurity topics essential to their career. Topics include, but are not limited to vulnerabilities, threats, and controls associated with systems, networks, and information assets. Offensive security [3,4,11] are taught in providing CJ professionals with comprehensive knowledge of cybercrimes. Hands-on lab activities [12, 13] and scenario-based learning [14] are integrated to empower CJ professionals' abilities to apply fundamental cybersecurity knowledge into practice. This course lays a foundation for further learning in the second and third courses.

Course 2, Cyber Forensics and Cyber Intelligence, aims to enable CJ professionals to handle law and technology-related civil and criminal matters by utilizing current and emerging technologies in cyber forensics and incident response. The most vital aspect of this course is integrating artificial intelligence (AI) training [15,16,17] through web-based labs, showcasing real-world examples of AI in action. CJ learners are engaged with AI systems and explore its practical applications for addressing cybercrime. Interactive simulations and case studies foster critical thinking, ethical decision-making, and an understanding of the societal implications of AI in addressing cybercrime. Topics include Ethical considerations in AI, AI and cybersecurity, AI and privacy protection, and AI and social media as shown in Figure 2.

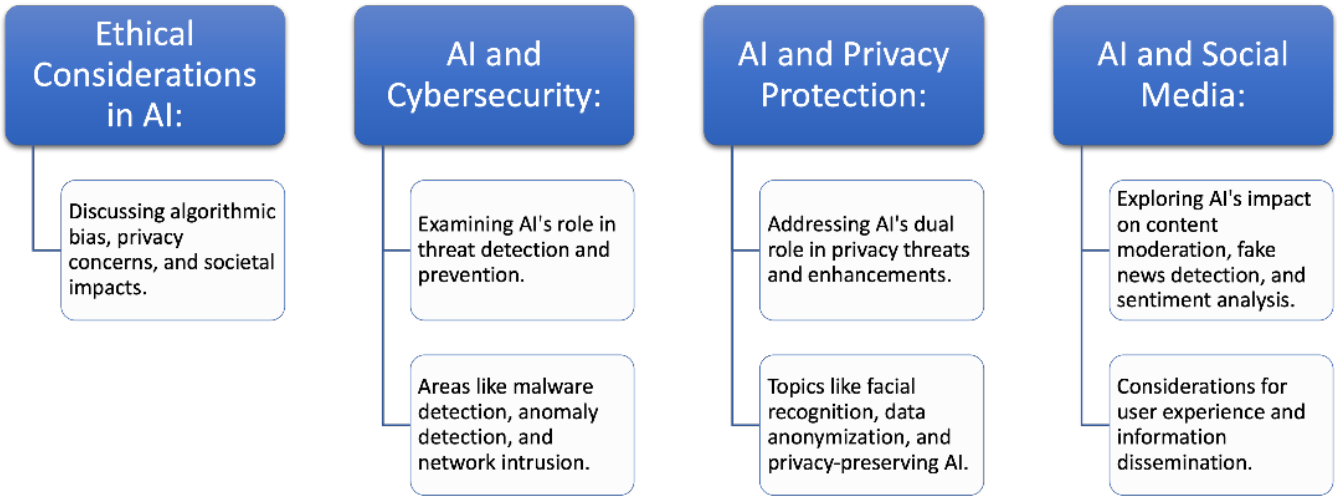


Fig. 2. Topics in cyber intelligence.

Course 3, Cyber Challenges in Criminal Justice, builds upon course 1 and course 2, by addressing specific cyber challenges faced in the CJ field. By solving real-world challenges [18], CJ professionals gain practical experience and deepen their knowledge of forensic analysis of cybercrime, security and privacy management, and the use of AI technologies for addressing cybercrime.

IV. EXAMPLE COURSE MODULES

Example course modules that have been used in our courses are presented in this section.

In course 1, four modules, Introduction to Cybersecurity, Computer Security, Internet Security, and Privacy, are developed. The first module, Introduction to Cybersecurity, provides an overview of cybersecurity concepts and fundamental principles. The other three modules cover other important topics in different security domains. Each module consists of concepts explained, web-based labs, and case studies. Web-based labs provide learners with hands-on activities to enhance their learning of cybersecurity concepts and principles. Case studies describe real world cybercrime scenarios. Through analysis and discussions about real life cyber examples, CJ professional learners gain practical experience that can be applied when solving the cyber problems they will face throughout their careers.

In course 2, five modules, Introduction to AI and Cybersecurity, Unsupervised Learning for Cybersecurity, Supervised Learning for Cybersecurity, Generative AI, Ethical Considerations in AI for Cybersecurity, are developed. The first module, Introduction to AI and Cybersecurity, provides an overview of the intersections of cybersecurity and AI. The other four modules cover the important applications of AI technologies for cybersecurity. Like course 1, each module consists of concepts explained, web-based labs, and case studies.

Course 3 (Cyber Challenges in Criminal Justice) demonstrates AI in Cybersecurity, leveraging ChatGPT. In course 3, three case studies in using ChatGPT to identify data loss, assist access control, and aid fraud detection are developed. All the three case studies are good examples of internet-related cybercrimes that are closely connected to the main types of cybercrimes involved in the criminal justice systems.

We highlight some key parts of our course design and activities in the following.

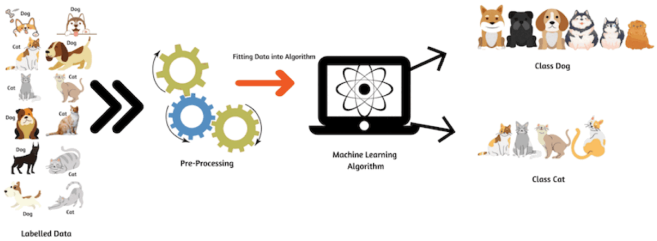
A. Interactive Simulations for Concepts Explained

To engage CJ learners with cybersecurity lessons, we have developed interactive simulations to explain key cybersecurity and AI concepts and allow them to practice relevant skills. Below is an example lesson teaching the concept of supervising learning to novices. In the lesson, we first explain what supervising learning is, then we ask the learners to use the interactive simulations, so they become familiar with the concept of supervising learning.

As shown in Figure. 3 (b), we used an interactive simulation to demonstrate that a supervising learning algorithm could be trained to identify images of cats and dogs by being fed an ample amount of training data that would consist of different labeled images of cats and dogs. This training data would be a subset of photos from a much larger data set of images. After training, the model should then be capable of predicting if an output of an image is either a cat or a dog. Another set of images can be run through the algorithm to validate the model.

Supervising learning is when a computer learns by practicing with examples that are already marked with the right answers. It's like a practice test where every question comes with the correct answer, so the computer can learn the pattern. After practicing, the computer is given a real test with questions it hasn't seen before. The answers are there but hidden from the computer, to check if it has learned well enough to figure out the answers on its own. This real test helps to see if the computer can now make good guesses without being told the answers.

(a) Concepts Explained: Supervising learning



(b) Illustration of Supervising learning Using Interactive Simulation

Fig. 3. Example lesson about supervising learning.

B. *Web-based labs*

We have adopted and developed web-based labs in Course 1 and Course 2 to enhance CJ learners' understanding of Cybersecurity and AI concepts and abilities to apply knowledge about Cybersecurity and AI in CJ fields. Specifically, Course 1 includes seven cybersecurity labs: 1) *Risk Management* lab in which students practice threat identification, risk analysis and risk mitigation in a real-world scenario; 2) *Anatomy of a Ransomware Attack* lab in which students gain insight into how a ransomware attack occurs and learn strategies to counteract it; 3) *Virus Attack* lab in which students engage in interactive role-play scenarios to simulate virus attacks, enhancing their understanding of how such attacks occur in various contexts. 4) *Scam* lab in which students practice identifying scam email attempts to raise awareness and equip them with the skills needed to detect and avoid email scams; 5) *Malware Animation* lab in which students visualize twelve distinct types of malware, including viruses, worms, trojans, remote access trojan, logic bombs, keylogger, spyware, adware, botnets, rootkits, advanced persistent threats and zero-day attacks, to enhance their understanding of the significant impact of malware; 6) *Advanced Encryption Standard (AES)* lab in which students learn how AES encryption and decryption work through interactive web demonstrations; and 7) *Hash Functions* lab in which students explore the encoding and decoding processes of various hash functions to deepen their understanding of the role of hashing in cybersecurity.

Course 2 includes five labs in AI: 1) K-Means Clustering simulation. In this K-Means Clustering simulation, students visualize the K-means algorithm to grasp how data is grouped and categorized. This lab offers clear and intuitive insight into clustering techniques in AI; 2) Spam Email Detection. In this lab, students engage in hands-on exercises to explore AI's ability to detect spam emails; 3) Quick Draw by Google. Students interact with Google's Quick Draw tool to experience AI-assisted drawing. This activity showcases how AI creatively interprets and predicts user input; 4) Facial Recognition. Students discover the principles behind facial recognition technology through interactive demonstrations; and 5) Phishing Campaigns. This lab simulates phishing campaigns and evaluates user responses by generating survey pages using OpenAI Chat. It emphasizes AI's role in analyzing and improving phishing awareness.

Below are the two lab examples. Each lab consists of lab description followed by lab activity.

1) *Lab Example 1: Spam Email Detection - Text Machine Learning*

a) *Lab Description*

Spam email detection identifies and filters out unwanted emails. It analyzes the content of incoming emails and looks for patterns and signals that are commonly associated with spam, like certain keywords or suspicious links. Machine Learning, such as, Support Vector Machines (SVM), learns from examples of spam and non-spam emails and gets better over time at identifying spam. A simplified explanation of how SVM works, using an analogy, is presented in the following.

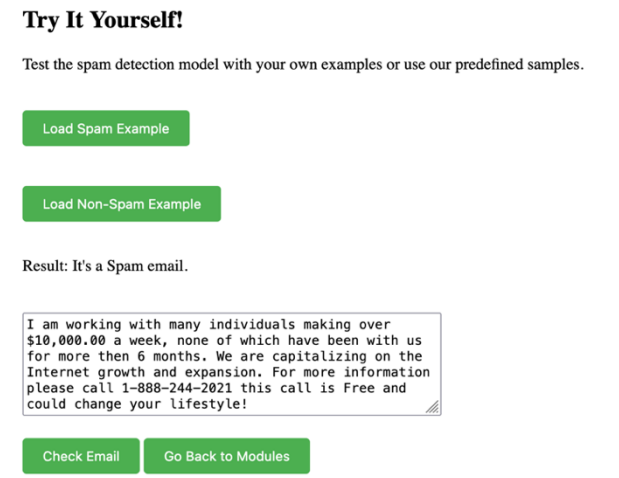
Imagine you're at a party and you're tasked with separating the partygoers into two groups: those who like to dance and those who prefer to sit. You notice that there are some obvious differences in clothing style, energy levels, and whether they're already dancing or not. Your job is to draw a line on the ground that separates the dancers from the non-dancers. In machine learning terms, this line is called a hyperplane and the attributes you use to distinguish the groups (clothing style, energy level, dancing state) are called features.

Just like you observed partygoers' characteristics, SVM looks at emails and extracts features. This could be the presence of certain keywords that are often found in spam, the frequency of those words, the sender's email address, or even the time the email was sent. Once the features are extracted, the SVM is trained with a dataset of emails that are already labeled as spam or non-spam. This is like you learning from observing a few parties and identifying which kinds of behaviors typically indicate a preference for dancing. The SVM algorithm tries to find the hyperplane that best separates the spam emails from the non-spam emails. This is like drawing the best line on the floor of the party that separates dancers from non-dancers, which maximizes the distance (margin) from the line to the nearest partygoers of any group. After the hyperplane is established, when a new email comes in, the SVM checks which side of the hyperplane the email falls on, based on its features. If it lands on the side with spam emails, it is classified as spam; if it lands on the side with non-spam emails, it is classified as non-spam. Think of it as watching where a new guest goes when they arrive at the party — if they

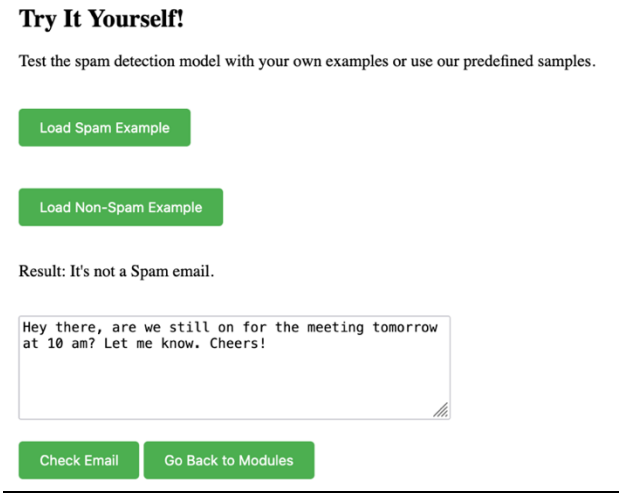
head for the dance floor, you'd classify them as a dancer; if they head for the seats, you'd classify them as a non-dancer.

b) Lab Activities

Test the spam detection model with your own email examples or use our predefined email samples. Below are the two sample screenshots of spam detection.



(a) Spam email



(a) Non-Spam email

Fig. 4. Spam detection lab based on Support Vector Machines (SVM).

2) Lab Example 2: Face Recognition - Image Machine Learning

a) Lab Description

Facial recognition technology is a method for identifying or verifying the identity of an individual using their face. It captures, analyzes, and compares patterns based on the person's facial contours. Think of facial recognition like a skilled artist drawing a portrait. Just as an artist observes and captures unique features like the distance between eyes or the shape of the chin, facial recognition software maps out "facial landmarks": each face's distinct characteristics. It then creates a digital "sketch" or a mathematical formula of these features. Facial recognition runs on image machine learning. Imagine machine learning as teaching a child to distinguish different types of fruit. By showing them various fruits multiple times, they learn to recognize each one. Similarly, we "teach" the computer by feeding it many images, helping it learn to identify and differentiate faces.

Facial recognition technology typically employs Convolutional Neural Networks (CNNs), a type of deep learning model particularly well-suited for processing and analyzing visual imagery. CNNs in Facial Recognition consist of Image Processing (i.e., using filters to capture different aspects of an image, such as edges, shapes, or texture), Feature Extraction (i.e., analyzing facial features by detecting specific patterns and variations in a face, such as the distance between eyes, the shape of the nose, the contour of the jawline, etc.), Layered Architecture (i.e., using hierarchical structure enables the network to gradually learn more detailed aspects of the data, from basic features like edges or colors, to more complex features), Training with Large Datasets to improve the model's accuracy in recognizing faces, and Classification and Matching by comparing the facial features of new images with the data it has learned.

b) Lab Activities

Perform face recognition with your own images. Below is a sample screenshot of face recognition.

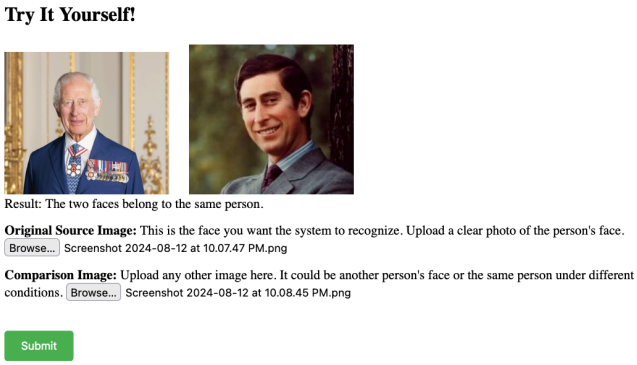


Fig. 5. Face Recognition Lab [19, 20].

C. Case Studies

We have selected some case scenarios from NIST (National Institute of Standards and Technology) and developed case studies about some important topics in cybersecurity and AI, which help CJ learners gain real-world experience in applying cybersecurity and AI knowledge and skills in handling cybercrime. Below is a case study example. It consists of case description, learning objectives, and activities.

Through this case study, CJ Professionals can integrate what they have learned in Internet Security into practice, including, but not limited to the concept of digital evidence, internet layers, internet security risks, and internet defenses.

Case Description: ABC Company is a small manufacturing firm that recently was the victim of a devastating cyberattack that disrupted its operations and eroded their customers' trust. On a mundane morning, employees arrived at work where their computers were unresponsive and displaying a worrying message: "Your Data Has Been Compromised". It soon became clear that ABC had fallen victim to a sophisticated cyberattack targeting its customer database and website. The attackers had accessed their network and stolen sensitive customer data, including names, phone numbers, addresses, email addresses, and credit card information. Years of client records had been compromised, representing a significant breach of privacy and trust. Beyond the data, ABC's website had also been defaced; attackers had replaced ABC's homepage with a cryptic message mocking their inadequate security defenses. In the aftermath, ABC faced questioning from clients, authorities, and media. ABC incurred significant financial losses due to the cyberattack: expensive lawsuits, regulatory fines, and compensation claims from affected consumers.

(a) Case description

Learning Objective: Analyze a real-world cybercrime example and apply Internet Security concepts and principles in protecting digital information and systems from unauthorized access, data breaches, and network threats, and maintaining public safety in the digital realm.

Activities: Discuss the following questions.

1. What were the initial indicators of the cyberattack? What specific customer information was compromised in the attack?
2. How has the cyberattack impacted ABC Company's finances?
3. What security vulnerabilities were exploited by the attackers? What countermeasures against these types of attacks are available?
4. What are the legal implications of the attack and data exposure for ABC Company?

(b) Case study objectives and activities

Fig. 6. Case Study Example

V. CONCLUSION

To address the challenges that we identified through literature reviews and focus group surveys in cybersecurity education for CJ professionals, we develop a learning pathway consisting of three progressive cybersecurity courses. These courses using interactive simulation, web-based lab, case studies, and challenging projects targeting CJ educators and practitioners. The curriculum is developed based on interdisciplinary efforts among Cybersecurity and AI experts and CJ professionals. It can not only effectively solve the problems of lacking effective cybersecurity education (courses and programs) in the CJ fields, shortage of innovative and practical training for CJ professionals, unavailable instructional resources, experts, and time in both cybersecurity and CJ, but also foster strategical partnership among communities of cybersecurity, AI and CJ, in keeping up with evolving cyber technologies to deal with modern complex cybercrime. An ongoing work is to conduct a pilot training for CJ professionals using the developed curriculum. We will then assess the course contents, lessons, and activities by surveys and interviews from the pilot study group to revise our training curriculum.

ACKNOWLEDGEMENT

This research was, in part, supported by National Science Foundation (NSF) Grants 2334196 and 2334197. We thank Yudu Li for assisting in surveys, Kimia Tuz Zaman, Wordh Ul Hasan, Rakibul Hasan Nahid, Michelle Crosby, Ryan Enyeart-Yoiungblood, Nikita Johnson, Kari Stephenson, Shubing Yang, and Allan France, for their contributions in the course development, and reviewers' valuable suggestions for improving this paper.

REFERENCES

[1] Hulatt, D., Stavrou, E. (2021). The Development of a Multidisciplinary Cybersecurity Workforce: An Investigation. In: Furnell, S., Clarke, N. (eds) Human Aspects of Information Security and Assurance. HAISA 2021. IFIP Advances in Information and Communication Technology, vol 613. Springer, Cham. https://doi.org/10.1007/978-3-030-81111-2_12.

[2] Sample, Char; Loo, Sin Ming; Justice, Connie; Taylor, Eleanor; and Hampton, Clay. (2020). "Cyber-Informed: Bridging Cybersecurity and Other Disciplines". Proceedings of the 19th European Conference on Cyber Warfare and Security, ECCWS 2020, 334-341.

[3] A. Aibekova and V. Selvarajah, "Offensive Security: Study on Penetration Testing Attacks, Methods, and their Types," 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), Ballari, India, 2022, pp. 1-9, doi: 10.1109/ICDCECE53908.2022.9792772.

[4] A. B. Ajmal, M. A. Shah, C. Maple, M. N. Asghar and S. U. Islam, "Offensive Security: Towards Proactive Threat Hunting via Adversary Emulation," in IEEE Access, vol. 9, pp. 126023-126033, 2021, doi: 10.81109/ACCESS.2021.3104260.

[5] L. Hadlington, K. Lumsden, A. Black, and F. Ferra, "A Qualitative Exploration of Police Officers' Experiences, Challenges, and Perceptions of Cybercrime," Policing-A journal of policy and practice, vol. 15, no. 1, pp. 34–43, Mar. 2021, doi: 10.1093/POLICE/PAY090.

[6] A. M. Bossler and T. Berenblum, "Introduction: new directions in cybercrime research," J Crime Justice, vol. 42, no. 5, pp. 495–499, Oct. 2019, doi: 10.1080/0735648X.2019.1692426.

[7] L. Hadlington, K. Lumsden, … A. B.-P. A. J. of, and undefined 2021, "A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime," academic.oup.com, Accessed: August 12, 2024. [Online]. Available: https://academic.oup.com/policing/article-abstract/15/1/34/5233865.

[8] A. M. Bossler and T. J. Holt, "Patrol officers' perceived role in responding to cybercrime," Policing, vol. 35, no. 1, pp. 165–181, Mar. 2012, doi: 10.1108/13639511211215504.

[9] J. Nosál, "Crime in the Digital Age: A New Frontier," The Implications of Emerging Technologies in the Euro-Atlantic Space, pp. 177–193, 2023, doi: 10.1007/978-3-031-24673-9_11.

[10] A. Reyes, K. O'Shea, J. Steele, J. R. Hansen, B. R. Jean, and T. Ralph, "Cyber crime investigations: Bridging the gaps between security professionals, law enforcement, and prosecutors," Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors, pp. 1–412, Mar. 2007, doi: 10.1016/B978-1-59749-133-4.X5000-1.

[11] A. B. Ajmal, S. Khan, M. Alam, A. Mehbodniya, J. Webber and A. Waheed, "Towards Effective Evaluation of Cyber Defense: Threat Based Adversary Emulation Approach," in IEEE Access, doi: 10.1109/ACCESS.2023.3272629.

[12] W. Du, "SEED: Hands-On Lab Exercises for Computer Security Education," in IEEE Security & Privacy, vol. 9, no. 5, pp. 70-73, Sept.-Oct. 2011, doi: 10.1109/MSP.2011.139.

[13] Z. Zeng, Y. Deng, I. Hsiao, D. Huang and C. -J. Chung, "Improving student learning performance in a virtual hands-on lab system in cybersecurity education," 2018 IEEE Frontiers in Education Conference (FIE), San Jose, CA, USA, 2018, pp. 1-5, doi: 10.1109/FIE.2018.8658855.

[14] D. Lee, D. Kim, C. Lee, M. K. Ahn and W. Lee, "ICSTASY: An Integrated Cybersecurity Training System for Military Personnel," in IEEE Access, vol. 10, pp. 62232-62246, 2022, doi: 10.1109/ACCESS.2022.3182383

[15] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat and T. R. Gadekallu, "A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions," in IEEE Access, vol. 10, pp. 11065-11089, 2022, doi: 10.1109/ACCESS.2022.3142508.

[16] A. Singh, N. Singh, S. K. Singh and S. k. Nayak, "Cyber-Crime and Digital Forensics: Challenges Resolution," 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2023, pp. 1-7, doi: 10.1109/ICCCI56745.2023.10128333.

[17] C. Balarengadurai, D. C D and H. C, "Survey on Cyber Crime Problems and Prevention," 2022 International Conference on Smart and Sustainable Technologies in Energy and Power Sectors (SSTEPS), Mahendragarh, India, 2022, pp. 117-121, doi: 10.1109/SSTEPS57475.2022.00039.

[18] Z. Trabelsi, S. Zeidan and H. Saleous, "Teaching Emerging DDoS Attacks on Firewalls: A Case Study of the BlackNurse Attack," 2019 IEEE Global Engineering Education Conference (EDUCON), Dubai, United Arab Emirates, 2019, pp. 977-985, doi: 10.1109/EDUCON.2019.8725133.

[19] Official Australian Portraits of The King and Queen, https://www.npg.org.uk/collections/search/person?LinkID=mp05145&wPage=7&_gl=1. Accessed: August 12, 2024.

[20] Canadian Royal Portraits, https://www.canada.ca/en/canadian-heritage/services/royal-portraits.html, Accessed: August 12, 2024.

[21] B.K. Payne and L. Hadzhidimova, “Cyber Security and Criminal Justice Programs in the United States: Exploring the Intersections”, International Journal of Criminal Justice Sciences, Vol. 13, Issue 2, 2018, pp. 385-404.

[22] Ofusori, L., Bokaba, T., & Mhlongo, S. (2024). Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction. Applied Artificial Intelligence, 38(1). https://doi.org/10.1080/08839514.2024.2439609

[23] L. Ho, S. Rabiei, and D. White, “A Comparative Study of Interdisciplinary Cybersecurity Education”, Part of the UC Berkeley Center for Long-Term Cybersecurity White Paper Series, Sept. 2023, Accessed: December 26, 2024. [Online].Available: https://cltc.berkeley.edu/publication/interdisciplinary-cybersecurity-education/.

[24] J. Prümmer, T. Steen, and B. Berg, “A Systematic Review of Current Cybersecurity Training Methods”, Computers & Security, Vol. 136, 2024,103585,ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103585.