Issues in Information Systems
Volume 25, Issue 3 pp. 109-118, 2024

DOI: https://doi.org/10.48009/3_iis_2024_109

Embedding AI competencies in a cyber security graduate program: identifying existing gaps

Sushma Mishra, *Robert Morris University*, *mishra@rmu.edu*
Nooredin (Noory) Etezady, *Robert Morris University*, *etezady@rmu.edu*

Abstract

Cybersecurity threats have become complex and challenging to mitigate. Integrating Artificial Intelligence (AI) competencies into the cybersecurity curriculum is essential to develop a workforce capable of addressing contemporary security challenges. This paper proposes a comprehensive conceptual model designed to map AI competencies onto graduate curricula in cybersecurity. The model uses AI competencies (managerial and technical) to assess its presence within an existing MS cybersecurity program in different courses. The results suggest that while managerial AI competencies—such as strategic implementation, governance considerations, and communications—are well-represented and thoroughly integrated, there is a gap in including technical AI competencies. These technical competencies include advanced machine learning techniques, algorithm development, and hands-on AI tool application. Our findings highlight the need for curriculum developers to enhance cybersecurity curricula' technical AI training components. Implications are noted, and future research directions are suggested.

Keywords: artificial intelligence, machine learning, cybersecurity, curriculum, graduate program, model skills gap

Introduction

Cybersecurity is an essential functionality across various sectors as it fulfills the basic need of maintaining the integrity, confidentiality, and availability of information across organizations. As cyber threat vectors become increasingly sophisticated, the need for cybersecurity professionals has never been greater. Department of Labor statistics show that 700,000 jobs in cybersecurity are not filled in the United States (Wu, 2024). The emergence of Artificial Intelligence (AI) is rapidly changing traditional ways of doing things in many sectors, including cybersecurity. AI can analyze extensive datasets, detect patterns, and predict potential threats, making cybersecurity solutions more effective (Wong et al., 2024).

Embedding AI competencies within the cybersecurity curriculum addresses several critical industry needs. The cybersecurity industry is increasingly using AI in its solutions, and incorporating these concepts in the curriculum will allow graduates to have relevant skills to meet the challenges of the workforce. The notable skills gap in the cybersecurity workforce (Wu, 2024) could be reduced by training graduates in ways that increase their employability.

The emergent nature of risks and threats in today's world requires innovative cybersecurity solutions. Traditional cybersecurity approaches in academia are foundational and often fail to leverage cutting-edge technologies such as AI. Learning cybersecurity through the lens of AI could offer multiple advantages to organizations in enhanced user authentication, behavioral analytics (Wong et al., 2024), and adaptive

security policies (Fortinet, 2024), to name a few. However, to fully exploit these advantages, the future generation of cybersecurity experts must be experts in cybersecurity principles and AI technologies.

The cybersecurity workforce needs to be educated in AI technologies in addition to cybersecurity principles. To prepare the future cybersecurity workforce, universities, and colleges need to incorporate AI competencies into their existing cybersecurity programs. This study attempts to answer the following two questions:

1. *What AI competencies are required for inclusion into existing cybersecurity programs?*
2. *How should the identified AI competencies be incorporated into cybersecurity programs?*

To answer these questions, a comprehensive literature review is conducted. The required AI competencies for cyber security programs are identified. Then, a comprehensive framework for integrating AI competencies is proposed based on guidelines from prior research. Finally, the proposed framework is demonstrated by applying it to the cybersecurity curriculum of a Master of Science (MS) program at a small private university in the Northeastern part of the United States. This integration is designed to equip students with the skills to address contemporary cybersecurity challenges effectively.

The rest of this paper is organized as follows. This introduction section is followed by an extensive literature review showing a need for a curriculum integrating AI and cybersecurity. The proposed conceptual framework and discussions are presented. Implications are noted, limitations are discussed, and conclusions and future research are presented.

Literature Review

Artificial Intelligence (AI) is a popular concept that uses mathematical algorithms to conclude basic facts about events and their impacts. AI attempts to create automated intelligence, which is similar to human intelligence. AI can utilize massive data and computing to learn and can be utilized in three ways (Moravat & Panda, 2020):

- Assistance intelligence to enhance the tasks that people perform,
- Augmented intelligence to enable its users to perform tasks that they could not perform before and
- Autonomous intelligence refers to acting by itself without a human operative.

AI, therefore, attempts to address challenging problems. Cybersecurity has become a big problem because of the growing sophisticated nature of cyber-attacks, which continuously result in colossal productivity and financial loss for organizations worldwide.

As Naik, Mehta, Yagnik, and Shah (2022) noted, the security measures employed are not satisfactory to protect information systems from various cyber threats. Cyberdefense systems need to quickly identify real threats by analyzing the input data from various cybersecurity defense tools and making real-time decisions in response when necessary. As Wei-Kocsis, Sabounchi, Mendis, Fernando, Yang, and Zhang (2023) noted, the growth of AI, especially machine learning, has a significant effect on increasing awareness, real-time reaction, and enhancing the general effectiveness of autonomous and semi-autonomous security systems. AI employs various techniques, such as expert systems, intelligent agents, deep learning, machine learning, speech recognition, text analysis, and natural language generation and processing, to train machines to simulate human skills. These techniques can be integrated into cybersecurity defense. AI applications adapt to their usage, are self-directed, harmonize, diagnose, and self-learn, which can significantly contribute to cybersecurity. AI can be used in data mining, pattern identification, predicting future events and detection

processes, issuing warnings, and possibly taking the required cybersecurity measures to stop attacks before occurring (Chakraborty et al., 2022; Naik et al.).

A workforce skilled in AI is needed to implement AI and conduct daily business. However, there is a shortage of AI skills for AI implementations and operations (Brock & von Wangenheim, 2023; Anton et al., 2020). Wei-Kocsis et al. (2023) noted that despite the significant AI research progress in understanding the trust and security of AI techniques, the education and training needed to develop a cyber workforce that understands the AI technologies, usefulness, limitations, and best practices are lacking. Not having an AI-educated workforce will choke AI advancement and exacerbate the cybersecurity workforce shortage.

According to Rigi et al. (2022) in the report by the Joint Research Centre (JRC), the European Commission's Science and Knowledge Service, when comparing masters in AI and cybersecurity as a proportion to all offered masters, the EU offers more master's programs in AI, cybersecurity, and specialized masters (e.g., AI in the areas of Information and communication technologies; Business, administration, and law) than the US. Regarding the number of computer security master programs offered in cybersecurity programs, the US leads the EU and the United Kingdom. According to the report, the US had 537 cybersecurity masters and 293 specialized masters (e.g., cybersecurity in Information and communication technologies, Business, administration, and law) in 2020-2021. The cybersecurity content areas primarily taught in the US are Data Security and privacy and Network and distributed Systems. The report above does not indicate the incorporation of AI in cybersecurity education, whether in the US or elsewhere.

Various professions must acquire or strengthen the necessary AI competencies to address the challenges of developing modern information systems. Nevertheless, the focus on these AI competencies is lacking (Anton et al., 2020). As Jackson, Matei, and Bertino (2023) noted, the advent of AI has challenged educators, researchers, students, and practitioners to reconsider their curricula, questions, learning styles, and procedures. Graduate students are greatly concerned about the disconnect between education and practice. They are apprehensive about their education being in step and suitable to the latest AI-driven developments in cybersecurity. The rapid development of AI tools and the complexity of cybersecurity threats force cybersecurity educators to reassess how and what they teach. DeBello, Troja, and Truong (2023) also noted that higher education cybersecurity programs have not been updated with the latest research and methods on Artificial Intelligence cybersecurity.

As Alammari, Sohaib, and Younes (2022) noted, a dynamic mix of knowledge, skills, and abilities makes up cybersecurity competencies. Cybersecurity knowledge alone does not guarantee success in cybersecurity. Human abilities and technical skills are needed for a successful practicing cybersecurity professional. Jackson et al. (2023) found that effective communication is required to explain cybersecurity threats and solutions in layperson terms for complex issues such as AI and cybersecurity.

AI Competency Framework

AI proficiency is required for AI adoption. A lack of AI-skilled workers necessitates a guideline for organizations to understand and encourage AI-required competencies (Smith & Neupane, 2018). Anton et al. (2020) developed a comprehensive AI competency framework to leverage AI effectively. The competency framework was developed following a three-step process, which included qualitative content analysis, quantitative content analysis, and method and data triangulation. The first step involved the qualitative content analysis of relevant peer-reviewed publications obtained from interdisciplinary scholarly databases to identify necessary human skills across domains and AI-associated technologies. This step was

performed as a systematic literature analysis to establish the theoretical perspective for their research considering the technological advancements, AI investments, and publication volume of AI papers (Anton et al.). In the second step, quantitative content analysis of job advertisements from 60 countries was performed to scrutinize the practical view and evaluate the previous step. In the third step, method and data triangulation, the qualitative and quantitative content analysis methods were triangulated by integrating their results. Triangulation, a common approach for mixed methods research, provides a multi-perspective view when examining a research question. Subsequently, a complete overview of key technical and managerial competencies necessary for AI implementation and utilization on an individual level was presented. The authors proposed the following technical and managerial AI competencies.

Technical competencies

These core competencies are essential to solving a business problem using AI through technical and systems knowledge. It included knowledge in AI-associated technologies and algorithms (ML, deep learning, neural networks), programming (Python et al., web development), AI frameworks and libraries (TensorFlow et al., Scikit-learn, Numpy, Caffe), big data analytics frameworks (Spark, Hadoop); STEM knowledge (mathematical and statistical knowledge, computer science); development methodologies (Agile software development); problem-solving (initiative/engagement); data management (data management).

Managerial competencies

These competencies include business management (client focus/orientation, decision-making), business acumen (business development, interdisciplinary knowledge), people and social skills (collaboration, building trust, leadership), and communication (oral and written communication). These competencies complement the technical ones and help solve business problems.
The following section proposes a conceptual model for embedding AI competencies into cybersecurity curricula.

Proposed Conceptual Model

Cybersecurity programs need to be updated with AI knowledge to prepare a cybersecurity workforce that understands AI technologies and can employ them in the cybersecurity field. In this section the AI competency model for a cybersecurity graduate program is presented. The model's AI competencies are based on the guidelines for AI competencies developed by Anton et al. (2020) through qualitative and quantitative content analysis of the scientific and practical literature and examination of more than 9,000 job advertisements.

The AI competencies of the AI competency model, presented in Table 2, consist of the required core and complementary competencies. The required core competencies for AI, which are technical, as well as the complementary managerial competencies, which are the skills that enable a security professional to work with other organization members to keep the organization secure, are shown in table 2.
To show how to apply the proposed conceptual AI competency model, the graduate program in cybersecurity of a small private university in the Northeastern part of the United States is assessed for AI competency. The developed AI competency model is utilized to assess the graduate program. Once the program is assessed, its shortcomings are identified and the necessary steps can be taken to align the program with the required AI competencies. A description of the graduate program in cybersecurity is presented below.

Graduate Program in Cybersecurity

To show how to apply the proposed conceptual AI competency model, the graduate program in cybersecurity of a small private university in the Northeastern part of the United States was assessed for AI competency. The University's MS in cybersecurity is a new and successful program with solid enrollment. The courses are designed to provide both managerial and technical perspectives on cybersecurity. The curriculum consists of 10 courses, which are offered in 8-week formats. The program description suggests that it provides foundational and advanced technical knowledge and skills in cybersecurity domains. This program covers network security, operating systems security, cryptography, secure software development, digital forensics, cyber risk management, incident response, and continuity of operation. The interdisciplinary program combines technology with relevant human, legal, policy, and ethical aspects of cybersecurity to protect cyberinfrastructure and information assets systematically and holistically.
The program is 30 credits long and includes ten required courses. Table 1 provides a brief description of each course.

Table 1: A brief description of all required courses in MS in cybersecurity

Course name	Course Description
C1 Foundations of Cybersecurity	This course covers the fundamental concepts of the interdisciplinary field of cybersecurity by combining both technical and management aspects. Students analyze cyber threats and vulnerabilities and examine standard cybersecurity technologies and best practices. The cybersecurity tools, methods, and components are explored to protect networks, operating systems, and applications. The human, legal, privacy, and ethical aspects of cybersecurity are also examined. The idea is to prepare students for advanced concepts in cybersecurity.
C2 Foundations of Cyber Forensics	This course exposes the student to digital forensic investigations. It is about conducting, documenting, and presenting a digital forensics investigation, including a discussion of ethics for the Expert Witness/Investigator. The course overviews digital investigations and data recovery types, emphasizing data presentation techniques and chain-of-evidence procedures. It outlines proper documentation and reporting procedures for digital investigations.
C3 Operating Systems Security	This course demonstrates fundamental principles of securing operating systems. Students use specified steps or measures to protect the OS from threats, viruses, worms, malware, or remote hacker intrusions. Best practices are explored to configure operating systems to industry security standards and safeguard any computer assets capable of being stolen, edited, or deleted if OS security is compromised.
C4 Defending and Securing Networks	This course covers essential knowledge and skills to analyze network traffic and security threats and defend and secure computer networks. Course topics include a review of network security fundamentals, network traffic and signature analysis, securing network devices, wireless network security, intrusion detection and prevention systems (IDS/IPS), honeypots, firewalls, and network security policy and management.
C5 Applied Cryptography	This course presents the basic paradigms and principles of modern cryptography. It examines the inner workings of cryptographic primitives with formal definitions of security and precise assumptions to achieve guaranteed security. It covers private-key (symmetric) and public-key (asymmetric) cryptography in depth with supportive algorithms and protocols for encryption, message digest, digital signature, key distribution, etc. Students will learn how to reason about the security of cryptographic constructions and how to apply it to real-world applications.
C6 Software and Application Security	In this course, Students will learn how and why to incorporate security features into the design process for an application and will be introduced to common security threats for different application environments, including software, web applications, and mobile applications. Students will learn to analyze applications for security vulnerabilities through code review and various static and dynamic testing methods, as well as apply prevention techniques and countermeasures for known vulnerabilities. As the threat landscape for applications is constantly evolving, students will also learn to locate resources that are up to date to address emerging application security issues.

Course name	Course Description
C7 Cybersecurity Risk Management	This course examines risk management and its application to cybersecurity. It will help the student identify cybersecurity risks, evaluate those risks, and make risk-based decisions given organizational resource constraints. Students will learn foundational concepts in risk management and be introduced to risk management standards and approaches, both qualitative and quantitative, for risk analysis. This course aims to assist professionals in understanding risk management and enabling them to leverage those principles to make an organization more resilient to operational disruptions and other perils.
C8 Cybersecurity Strategy and Governance	Cybersecurity governance is the enterprise-wide phenomenon that maximizes IT benefits while emergent security risks are optimally managed in an organization's strategic planning. Widely used frameworks such as COBIT are discussed to give the student an integrated theoretical and practical perspective of technology and information systems governance, control, and assurance. Emphasis is on the critical control mechanisms that support achieving control objectives and preventing, detecting, and correcting undesired events through responsible uses of resources, appropriate management of risk, and aligning information technology with the organization. The course will emphasize the role of data governance in aligning security risks with the acceptable risk appetite of an organization.
C9 Special Topics in Cybersecurity	The primary goal of this course is to cover specialized or emerging topics in cybersecurity that are not covered elsewhere or need additional discussion in the Cybersecurity program. This course provides a gateway to introducing and reexamining emerging trends, technologies, threats, and research in the cybersecurity domain.
C10 Cybersecurity Capstone	This is the graduate program exit course for students to demonstrate their advanced proficiency in Cybersecurity with comprehensive knowledge, skills, and abilities for professional practice or certifications. The capstone course offers the following multiple project areas for students to choose one or more with the instructor's approval: (1) Complete a full research paper in Cybersecurity for a peer-reviewed conference presentation or publication; (2) Complete a comprehensive portfolio report based on a relevant internship or work experience; (3) Pursue and reflect on a reputable and advanced level professional security certification (e.g., CISSP/Associate, CISM, CEH, or GIAC certifications); (4) Complete a report of research and reflection on the participation experience in a well-recognized regional or national cybersecurity competition or conference.

AI Competency Assessment

The AI competency assessment for the university's graduate cybersecurity program was performed based on the proposed AI competency model, which is shown in Table 2. The AI competencies are shown in the first column of Table 2. The courses that were evaluated are shown in columns C1 through C10 of Table 2. The result of the AI competency assessment for the university's graduate cybersecurity program is also shown in Table 2. The detailed description of how the assessment was performed is shown below. Each course was reviewed based on the topics covered in the syllabus.
The evaluation used the following logic:

- If a course directly delivered an AI competency listed on the AI competency model, it was identified as a Primary (P) course with the relevant competency already embedded in the curriculum.
- If the course indirectly covered specific AI competencies, it is identified as secondary (S).

For example, under managerial competencies in Table 2, there is a sub-competency labeled "People and social skills – collaboration, building trust, leadership." The people management skills are direct highlights of C6 Risk Management and C7 Strategy and Governance, and also, in the final course, C10 students collaborate to finish their capstone project. This course primarily emphasizes the social skills of team building. It is mapped as a secondary competency for C9, an emerging topics course. Depending on the topic, this course could create some collaborative opportunities.

Table 2 – AI Competency Model and Evaluation

AI competencies	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
Technical Competencies										
AI-associated technologies algorithms - ML, deep learning, and neural networks										
Programming – Python, Java, web development, Scala						P				S
AI frameworks & libraries – TensorFlow, Pytorch, Keras, Scikit-learn, Numpy, Caffe									S	S
Big data analytics frameworks - Spark, Hadoop									S	
STEM knowledge – mathematical statistical knowledge, computer science		P	P		P				P	P
Development methodologies – Agile software development						P				
Problem solving – initiative/engagement	P	P	P	P	P	P	P	P	P	P
Data management – data management						P		S		
Managerial Competencies										
Business management – client focus/orientation, decision making							P	P		P
Business acumen – business development, interdisciplinary knowledge	P	P	P				P	P	S	P
People and social skills – collaboration, building trust, leadership						P	P	P	S	P
Communication – oral and written communication							P	P		S

P-Primary (covers the concepts directly); S=Secondary (understanding of the concepts is implied)

The courses that lack the required AI competencies need to be reviewed and those competencies added. For example, for C1—Foundations of Cybersecurity, lessons/assignments must be added to introduce AI-associated technologies such as ML, Deep Learning, and neural networks. As seen in the table above, row 1 is empty. No courses in this program address the technical concepts of AI in the curriculum. Given the nature of the courses, there are multiple opportunities for AI/ML techniques in several courses. In the technical competition domain, we identify various concepts already embedded in the existing courses. For example, programming is covered in two courses. AI frameworks are libraries that are not explicitly addressed in this course. However, AI frameworks are not currently addressed in any of the courses. In summary, managerial competencies are covered in multiple courses in various ways; however, technical competencies in AI are not being addressed systematically in this graduate program for cybersecurity. This cybersecurity program is not directly oriented towards AI competencies, so none of this mapping shows a weakness of the program.

Discussion

The proposed model identifies potential areas for embedding AI competencies in existing curricula of a Master's program in cybersecurity. AI tools provide a unique capability to address cybersecurity vulnerabilities in both technical and managerial domains. The proposed conceptual framework shows that many cybersecurity courses incorporate managerial competencies that allow students to have good exposure to business management, development, and social skills in the managerial domain. There are a variety of courses that address these competencies and groom the future workforce for solid management.

The conceptual framework shows that every managerial competency proposed in this framework is addressed multiple times in the program.
The framework shows that the courses adequately address some technical AI competencies. For example, problem-solving is addressed in all the courses in the program. The courses address problem-solving in various ways and are the program's cornerstone. Another technical competency, STEM knowledge, which entails using math and statistics, is also addressed in multiple courses. Most AI tools are mathematics and statistics, and a strong foundation of these concepts prepares students for the rigors of using AI in the work environment.

As a technical AI competency, programming is explicitly covered in at least one course, identified as primary in this mapping (C6). The capstone course assumes that students know programming and can use it in a project (secondary). More courses could use programming-based assignments and activities to strengthen student experience in this area. Data management is covered in the strategy and governance course. Students learn about data management frameworks and practices in the strategy governance course. Still, it is not technical, so the strategy course (C6) is identified as secondary in the mapping. These concepts are also covered in database courses and application security; hence, this course (C8) is primary in the mapping. These courses do not explicitly teach big data analytics and AI frameworks. However, some courses allude to these concepts in projects assigned to students. Two courses (C9 and C10) identify these technical competencies as secondary, but the depth of coverage varies with students and instructors. Finally, AI-related algorithms such as ML, deep learning, and neural networks are not taught in any of the courses in this program. One needs to acknowledge that this is not a shortcoming of the program as it is not geared towards AI competencies. However, there is an excellent opportunity to embed these tools in one or more courses to prepare cybersecurity professionals to use AI for better security.

The future of robust cybersecurity would involve the fundamental ability to implement and use AI solutions. Embedding AI concepts and competencies in cybersecurity programs would enable these programs to create a workforce ready on day one to deal with the complexity of the cyber world. There are many benefits in the cyber world of using AI tools. Some of these include better detection of anomalies in network traffic (Wu, 2024), enhanced automated response to detected threats (Wang, 2024), using analytics to predict future disruptions, better incident management by correlating alerts from multiple tools, automation of routine tasks such as log analysis/vulnerability scanning to name a few. Including AI concepts in the cybersecurity curriculum allows professionals to be proficient with the latest tools and technologies to deal with emergent threats proactively. Organizations must leverage AI capabilities to improve comprehensive security planning and risk posture.

This paper has implications for research and practice. It is one of the few studies that suggest ways to embed AI tools and techniques in cybersecurity curricula to better prepare cybersecurity students for the workforce. More research is required to guide the use of AI to enhance the cybersecurity curriculum. For practice, this research guides the use of prevalent AI tools in existing cybersecurity programs for comprehensive security. One limitation of this study is that it is based on a review of the curriculum of a single program. Future studies could investigate more programs in cybersecurity to assess a realistic picture of the state of the curriculum in the context of AI.

Conclusion

Integrating AI competencies into the cybersecurity curriculum is essential to develop a futuristic and robust cybersecurity workforce. Cyber threats continue to evolve in complexity and frequency, and using AI technologies allows for enhanced detection, prevention, and mitigation of threats. Cybersecurity

professionals need to be equipped with knowledge of machine learning, predictive analytics, and automated systems to ensure the confidentiality, integrity, and availability of digital infrastructures. This paper identified the required AI competencies for cybersecurity programs for preparing future cybersecurity workforce. An AI competency model was proposed and was applied to a university's graduate program in cybersecurity. A mapping of AI competencies with the existing curriculum of the cybersecurity graduate program shows that managerial AI skills are receiving more focus in cybersecurity education than technical AI skills. The managerial skills covered in this program include risk assessment, strategic planning and governance, and policy development, which are crucial for comprehensive cybersecurity practices in organizations. However, the technical competencies of AI need to be integrated rigorously to create a balanced security program. This paper suggests that integrating AI into cybersecurity education will ensure a balanced skill set in the workforce. Future research will study AI competency assessment of cybersecurity programs at other universities. Also, after embedding AI competencies in the courses that lack those competencies, cybersecurity program graduates who are employed need to be surveyed and the results analyzed to assess the quality of the cybersecurity programs that have embedded AI competencies according to the proposed model.

References

Alammari, A., Sohaib, O., & Younes, S. (2022). Developing and evaluating cybersecurity competencies for students in computing programs. *Peerj Computer Science 8:e827* https://doi.org/10.7717/peerj-cs.827

Anton, E., Behne, A., & Teuteberg, F. (2020). The Humans Behind Artificial Intelligence – An Operationalisation of AI Competencies. *Proceedings of Twenty-Eighth European Conference on Information Systems (ECIS2020).* https://aisel.aisnet.org/ecis2020_rp/141

Brock, J. K., & von Wangenheim, F. (2019). Demystifying AI: What Digital Transformation Leaders Can Teach You About Realistic Artificial Intelligence. *California Management Review, 61*(4), 110-134. DOI: 10.1177/1536504219865226

Chakraborty, A., Biswas, A., & Khan, A. K. (2022). Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation. *DOI:10.48550/arXiv.2209.13454*

DeBello, J. E., Troja, E., & Truong, L. M. (2023). A Framework for Infusing Cybersecurity Programs with Real-World Artificial Intelligence Education. *Proceedings of the 2023 IEEE Global Engineering Education Conference (EDUCON).* 10.1109/EDUCON54358.2023.10125138

Fortinet (2024). Role of Artificial Intelligence (AI) in Cybersecurity, Retrieved on 05/25/24 from: https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity

Jackson, D., Matei, S. A., & Bertino, E. (2023). Artificial Intelligence Ethics Education in Cybersecurity: Challenges and Opportunities: A focus group report. arXiv preprint arXiv:2311.00903.

Moravat, K., & Panda, B. (2020). A Survey of Artificial Intelligence in Cybersecurity. *Proceedings of 2020 International Conference on Computational Science and Computational Intelligence (CSCI).* https: //doi.org/10.1109/CSCI51800.2020.00026

Naik, B., Mehta, A., Yagnik, H., & Shah, M. (2022). The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review. *Complex & Intelligent Systems, 8*, 1763-1780. https://doi.org/10.1007/s40747-021-00494-8.

Righi, R., Lopez Cobo, M., Papazoglou, M., Samoili, S., Cardona, M., Vazquez-Prada Baillet, M. & De Prato, G. (2022). Academic Offer of Advanced Digital Skills in 2020-21. International Comparison, EUR 31043 EN, *Publications Office of the European Union*, Luxembourg, 2022, ISBN 978-92-76-51267-7, doi:10.2760/466727, JRC128844.

Smith, M. L. & Neupane S. (2018). Artificial Intelligence and Human Development: Toward a Research Agenda, White Paper, *International Development Research Centre*.

Wei-Kocsis, J., Sabounchi, M., Mendis, G. J., Fernando, P., Yang, B., & Zhang, T. (2023). Cybersecurity education in the age of Artificial Intelligence: A novel proactive and collaborative learning paradigm. *IEEE Transaction on Education (Early Access)*, doi: 10.1109/TE.2023.3337337.

Wong, H., Chaing, A. & Pugh, B. (2024). The Transformative Role of AI in Cybersecurity: Understanding Current Applications and Benefits, RStreet, Retrieved on 05/25/24 From: https://www.rstreet.org/commentary/the-transformative-role-of-ai-in-cybersecurity-understanding-current-applications-and-benefits/

Wu, M. (2024). Introducing the Cyber Jobs Dataset, CSET, Retrieved in 05/24/24 from: https://cset.georgetown.edu/publication/introducing-the-cyber-jobs-dataset/#:~:text=The%20International%20Information%20System%20Security,roles%20in%20the%20United%20States.