Designing A New Graduate Course on Artificial Intelligence for Cybersecurity

Ping Wang
Department of Computer and Information Systems
Robert Morris University
Pittsburgh, PA, USA
wangp@rmu.edu

***Abstract* — Artificial intelligence (AI) technologies and solutions are increasingly integrated into various applications and domains of studies. Generative AI (Gen AI) also has significant impacts and implications for the fast-growing field of Cybersecurity and cybersecurity education for workforce development. This research proposes the design of a new graduate master's level credit course to integrate AI into cybersecurity education. This new course explores the evolving impacts of artificial intelligence on the cybersecurity ecosystem. The course is intended for students to learn to identify and evaluate AI-powered cyber threats and attacks and their implications as well as to utilize AI-powered systems for enhancing cyber threat detection, incident response, security automation, vulnerability analytics, and security risk assessment. The proposed course design will summarize initial suggestions of main topics, outcomes, activities, and assessment criteria for implementation.**

***Keywords –** AI; cybersecurity; vulnerability; learning outcomes; assessment.*

I. INTRODUCTION

Artificial intelligence (AI) is a fast-growing, promising, inter-disciplinary and comprehensive technology solution supported by advanced computing, machine learning, data and knowledge representation, robotics, and optimization. With the strong potential to increase automation, efficiency and productivity, Generative AI (Gen AI) is increasingly adopted and used in various industries and fields of studies including Cybersecurity. Cybersecurity is also an increasingly critical area for national security and economic prosperity in the digital age due to rising and evolving cyber threats and risks. As a double-edged sword, Gen AI powered tools and solutions present opportunities for more efficient and effective cybersecurity measures such as in network traffic analysis and in cyber threat detection, risk assessment, and incident response, along with risks and challenges for cybersecurity in the case of malicious use of AI for more devasting cyber-attacks [1]-[3].

There are strong short-term and long-term demands for skilled workers in Cybersecurity around the world and especially in the United States that are projected to far outpace the average national job growth in the next decade [4][5]. Higher education is the main avenue expected for providing the pipeline of qualified professionals to meet the growing cybersecurity workforce demand. The U.S. National Centers of Academic Excellence in Cybersecurity (NCAE-C) designation program jointly sponsored by the National Security Agency (NSA) and Department of Homeland Security (DHS) is a national standard for reviewing, certifying, and maintaining high quality of cybersecurity education programs with rigorous and consistent requirements for program evaluation as well as up-to-date knowledge units (KUs) aligned to cybersecurity knowledge, skills, and abilities (KSAs) [6][7]. A recent global cybersecurity workforce study report shows that cybersecurity organizations and professionals need to keep up with AI as a major technology innovation in order to maintain and improve their efficiency and agility [8]. Therefore, cybersecurity education programs need to incorporate AI in the curriculum and course design. This study will briefly review relevant background and summarize the initial design of the proposed graduate AI for Cybersecurity course.

II. BACKGROUND

Gen AI solutions have the capacity to help cybersecurity professionals to detect, analyze, and defend against cyber threats and attacks. Specific to cybersecurity, large language models (LLMs) and generative security models of Gen AI bring the major benefits of early threat detection, efficiency and accuracy in vulnerability and threat analysis and risk assessment, automated incident response, preventive and secure software development, as well as efficient training of cybersecurity professionals [9][10]. Recent research on AI for Cybersecurity shows that Gen AI applications have the capacity and strengths to automate repetitive security tasks, speed up cyber threat detection, penetration testing and response, and improve the accuracy of countermeasures to address cyber vulnerabilities and risks [11]-[13]. Therefore, a new course on AI for Cybersecurity should cover the security benefits of Gen AI and its applications and models.

Gen AI can be a double-edged sword to Cybersecurity, which also brings risks, challenges, and limitations for cybersecurity solutions. Unauthorized and malicious users could use AI tools to generate code and launch more powerful and devastating attacks and exploitations targeting known vulnerabilities [1][14]. For legitimate users, Gen AI applications, such as ChatGPT, may provide misleading results or "hallucinations", which is a substantial limitation [14][15]. In addition, there are concerns with the security and privacy risks of Gen AI applications that may disclose private and confidential user data on public domains [3][14][16]. Therefore, a new course on AI for Cybersecurity should also reveal and address the risks and limitations of AI models and applications.

For pedagogical and educational effectiveness, a new course design should reflect the cognitive development process of different levels or stages of learning objectives in the updated

Bloom's taxonomy, which lays out the following 6 levels of progressive learning objectives and achievements [17]:

- Recall information, facts, terms, and basic concepts
- Describe and interpret facts and ideas to demonstrate comprehension
- Apply knowledge and techniques learned to solve problems in new situations
- Analyze information to identify causes, motives, and relationships
- Evaluate information or ideas based on certain criteria to make judgements
- Develop and propose new or alternative solutions

III. PROPOSAL

The proposed new course is a 3-credit course for a master's degree program in applied AI at an NCAE-C designated university in the United States. The new course focuses on the evolving impacts of AI on the cybersecurity landscape and teaches students to identify and evaluate AI-powered cyber risks and solutions. The specific learning outcomes are:

- Identify and describe AI-powered cyber threats and attacks
- Evaluate AI-powered cyber threats and attacks and security implications and solutions
- Identify and describe positive impacts of AI in cybersecurity
- Identify and apply AI-driven solutions, techniques, and tools for cybersecurity
- Evaluate secure development practices for protecting applications in the age of AI
- Assess and evaluate AI-powered cybersecurity risks and solutions.

For a graduate level course, it is important include more advanced level learning objectives of analysis, evaluation, and solution development in Bloom's taxonomy.

A variety of teaching and learning activities are suggested for this new course, including presentations, hands-on demos, discussions, and a comprehensive project assignment for problem solving. The project assignment includes progressive development of an initial project plan involving identification of AI-related cyber threats and risks, a midterm progress report, and a final report and presentation that are submitted for grading and assessment. The main assessment criteria for the project include problem description, analysis, and evaluation and discussion of proposed solutions, tools, and methods. Student presentations demonstrate their problem solving skills.

IV. CONCLUSION

This abstract presents preliminary research on proposing a new graduate course on AI for Cybersecurity. Future research will report the actual implementation, empirical data, and areas of improvements identified for the course design.

ACKNOWLEDGEMENT

This research is supported by a grant from the U.S. National Science Foundation (NSF) – NSF Grant ID 2234554.

REFERENCES

[1] S. Wilson, "Cybersecurity and artificial intelligence: Threats and opportunities," Contrast Security, 2023.

[2] B. Schneier, "The coming AI hackers," in The Cyber Projecct: Council for the Responsible Use of AI, Harvard Kennedy School, 2021.

[3] NIST/US Department of Commerce, "NIST Trustworthy and Responsible AI, NIST AI 600-1," July 2024. Available: https://doi.org/10.6028/NIST.AI.600-1

[4] U.S. BLS, "Occupational Outlook Handbook – Information Security Analysts," 2025. Available: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[5] M. Hogan et al., "Cybersecurity Workforce Data Initiative: Cybersecurity Workforce Supply and Demand Report," National Science Foundation, 2024. Available: https://ncses.nsf.gov/about/cybersecurity-workforce-data-initiative

[6] P. Wang, M. Dawson, K.L. Williams, "Improving cyber defense education through national standard alignment: Case studies," *International Journal of Hyperconnectivity and Internet of Things.* 2018, *2*(1), pp. 12-28.

[7] U.S. National Security Agency, "National Centers of Academic Excellence in Cybersecurity," Available: https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

[8] (ISC)2, "Global Cybersecurity Workforce Prepares for an AI-Driven World," 2024. Available: https://www.isc2.org/research

[9] A. Mamgai, "Generative AI with cybersecurity: friend or foe of digital transformation?". Available: https://www.isaca.org/resources/news-and-trends/industry-news/2023

[10] P. Wang and H. D'Cruze, "AI-Assisted Pentesting Using ChatGPT-4" In Advances in Intelligent Systems and Computing, vol 1456. Springer, 2024. Available: https://doi.org/10.1007/978-3-031-56599-1_9

[11] R. Kaur, D. Gabrijelcic, and T. Klobucar, (2023). "Artificial intelligence for cybersecurity: Literature review and future research directions, Information Fusion 97 (2023) 101804, pp. 1-29

[12] P. Wang and H. D'Cruze, "AI-Assisted Pentesting Using ChatGPT-4" In Advances in Intelligent Systems and Computing, vol 1456. Springer, 2024. Available: https://doi.org/10.1007/978-3-031-56599-1_9

[13] S. Temara, "Maximizing penetration testing success with effective reconnaissance techniques using ChatGPT," Research Square, 2023, pp. 1-10, DOI: https://doi.org/10.21203/rs.3.rs-2707376/v1

[14] M. Gupta, K. Aryal, and L. Praharaj, "From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy," in IEEE Access, vol. 11, 2023, pp. 80218-80245

[15] X. Zhan, Y. Xu, and S. Sarkadi, "Deceptive AI ecosystems: The case of ChatGPT," In ACM conference on Conversational User Interfaces (CUI '23), July 19–21, 2023, Eindhoven, Netherlands.

[16] World Economic Forum, "Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards", White Paper, January 2025. Available: https://reports.weforum.org/

[17] L.W. Anderson, and D.R. Krathwohl, A taxonomy for learning, teaching, and assessing, Boston: MA: Allyn and Bacon, 2001.