CyberAI: Knowledge Area Frameworks for Cybersecurity Programs in the Age of Artificial Intelligence

Siddharth Kaza
Towson University, Towson, MD, USA, skaza@towson.edu

Blair Taylor
Towson University, Towson, MD, USA, btaylor@towson.edu

Paul Wagner
University of Arizona, Tucson, AZ, USA, paulewagner@arizona.edu

Shankar Banik
The Citadel, Charleston, SC, USA, baniks1@citadel.edu

Seth Hamman
Cedarville University, Cedarville, OH, USA, shamman@cedarville.edu

Vincent Nestler
California State University, San Bernardino, San Bernardino, CA, USA, vnestler@csusb.edu

Eman El-Sheikh
University of West Florida, Pensacola, FL, USA, eelsheikh@uwf.edu

Md Sajidul Islam Sajid
Towson University, Towson, MD, USA, msajid@towson.edu

Sagar Samtani
Indiana University, Bloomington, IN, USA, ssamtani@iu.edu

Paige Flores
Towson University, Towson, MD, USA, pzaleppa@towson.edu

Yair Levy
Nova Southeastern University, Fort Lauderdale, FL, USA, levyy@nova.edu

Patrick Tague
Carnegie Mellon University, Pittsburgh, PA, USA, ptague@cmu.edu

ABSTRACT

The CyberAI Programs of Study (PoS) represent a pioneering step in integrating Artificial Intelligence (AI) with cybersecurity education. Sponsored by the U.S. National Science Foundation (NSF) and developed in collaboration with the U.S. National Security Agency's (NSA) National Centers of Academic Excellence in Cybersecurity (NCAE-C), the CyberAI initiative (www.towson.edu/cyberai) aims to produce a workforce adept in both cybersecurity skills and AI competencies. This paper presents the knowledge areas produced in collaboration with 200+ individuals, with two distinct programs of study – SecureAI, securing the lifecycle of AI, and AICyber – using AI tools and techniques in cybersecurity. A review highlighting the evolution of cybersecurity educational standards and the growing necessity of

interdisciplinary AI integration in higher education is presented. Further, this paper outlines the development and validation processes for new Knowledge Units (KUs) supporting these programs, presents findings from pilot implementations, and discusses a validation framework aligned with the U.S. National Institute of Standards and Technology (NIST) NICE Framework and the U.S. DoD Cyber Workforce Framework (DCWF) standards.

CCS CONCEPTS

\begin{CCSXML}

<ccs2012>

<concept>

<concept_id>10002944.10011122.10003459</concept_id>

<concept_desc>General and reference~Computing standards, RFCs and guidelines</concept_desc>

<concept_significance>500</concept_significance>

</concept>

</ccs2012>

\end{CCSXML}

\ccsdesc[500]{General and reference~Computing standards, RFCs and guidelines}**KEYWORDS**
CyberAI, Cybersecurity, Artificial Intelligence, Knowledge Units, Academic Standards

1 Introduction

Artificial Intelligence (AI) is revolutionizing every domain it touches, and cybersecurity is no exception. With the rise of generative AI, deep learning systems, and intelligent automation, both the attack surface and defense mechanisms in cybersecurity are undergoing rapid transformation. Consequently, the future cybersecurity workforce must possess foundational and advanced skills in AI to address the emerging challenges and leverage AI-enabled tools for offense and defense.

In response to this imperative, the U.S. National Security Agency's (NSA) National Centers of Academic Excellence in Cybersecurity (NCAE-C), in collaboration with the U.S. National Science Foundation (NSF), spearheaded the creation of two AI-focused cybersecurity programs: SecureAI and AICyber. These Programs of Study (PoS) incorporate novel Knowledge Units (KUs) that equip students with foundational knowledge that leads to competencies spanning cybersecurity fundamentals, AI governance, adversarial learning, and AI-driven security assessments. This paper presents the KUs and outlines the motivation, framework, development methodology, and validation mechanisms behind these novel KUs.

2 Literature Review

The evolving threat landscape and rapid integration of AI require the development of standards for post-secondary cybersecurity and AI (CyberAI) programs. Despite growing enrollment in cybersecurity programs, substantial discrepancies persist between what is taught and industry expectations and requirements [1]. Moreover, AI is increasingly embedded into technology, cybersecurity, and associated frameworks, yet lacks analogous standardized curricular units or validation mechanisms.

2.1 Cybersecurity and AI Competent Workforce

A workforce competent in cybersecurity and AI is critical to national security, economic competitiveness, and social trust. The global economy increasingly relies on digital infrastructure, data analytics, and autonomous systems. Reports from the World Economic Forum (WEF) [2] and U.S. Bureau of Labor Statistics (BLS) [3] predicted exponential growth in professionals skilled in cybersecurity, AI, and data governance. This growth exacerbates the existing workforce gap that is estimated at over 4.7 million globally [4] and over 500,000 within the U.S. [5]. Additionally, employers identify lack of skills, hiring freezes, budget cuts, employee burnout and turnover, and layoffs as challenges related to maintaining a competent workforce [2][4]. Further, ISACA [6] found that organizations identified the shortage of AI security skills as a strategic risk and that AI skills and training are increasingly essential [7].

The convergence of AI and cybersecurity in the workplace intensifies this need. AI systems are increasingly deployed in sensitive decision-making roles, such as fraud detection, access control, and behavioral analytics. These tasks carry high risks if compromised by adversarial attacks. The U.S. National Institute of Standards and Technology's (NIST) AI Risk Management Framework (RMF) [8] acknowledged that the risks posed by AI are unique in many ways including how AI systems are trained, complex deployments making maintenance and management challenging, and the socio-technical nature of AI systems. This requires professionals to understand cybersecurity and AI to be capable of designing secure algorithms, detecting AI algorithms, utilizing AI-enhanced tools in Security Operations Centers' (SOCs) daily activities, and ensuring responsible AI governance [9].

2.2 Guidelines in Cybersecurity Education

Cybersecurity curricular guidelines have emerged from academia, industry training, and government programs with minimal convergence. The NIST's National Initiative for Cybersecurity Education (NICE) Framework for Cybersecurity [10] the Knowledge, Skills, Abilities, and Tasks (KSATs) to bridge the needs of educators, industry, and practitioners. Due to confusion and similarities to Skills, the NICE framework and DCWF removed Abilities to include only Tasks, Knowledge, and Skills (TKSs) [11]. Additionally, the Cybersecurity Body of Knowledge (CyBOK) [12], Cybersecurity Curricula 2017 Guidelines [13], and European Cybersecurity Education and Professional Training: Minimum Reference Curriculum [14] provided additional guidelines from U.S. and international perspectives. Dkaidek and Rashid [15] conducted a comparative study of these frameworks to identify the strengths in global applicability, interdisciplinarity, and curriculum guidance. Further, Towhidi and Pridmore [16] suggested that using Bloom's taxonomy with the NICE Framework [10] can support the educational curriculum development. Despite these frameworks, challenges remain in standardizing cybersecurity

education. Mukherjee et al. [17] and Ismail et al. [18] identified curricula gaps across programs worldwide, particularly in the areas of experiential learning and socio-technical domains. The imbalance between theoretical and hands-on skills impacts graduate employability and employer satisfaction [19].

2.3 AI Education: Emerging Needs and Gaps

AI capabilities have transitioned from niche technologies to essential workplace tools and are increasingly integrated into corporate and consumer technologies. Institutions increasingly develop and integrate AI programs and curricula to respond to employer demand, and students increasingly view AI literacy and responsible use as critical for career preparedness [20]. AI literacy is the ability to understand, use, monitor, and critically reflect on AI applications.

There are many approaches to integrating AI into current educational constructs. Southworth et al. [21] recommended integrating AI literacy across disciplines throughout K12 and post-secondary education as a minimum learning outcome. Additionally, Walter [22] promoted developing skills in prompt engineering, AI literacy, and the cultivation of critical thinking skills as crucial for education. In response, institutions are adopting policies [23] and exploring hybrid programs and certificates in applied AI and those that integrate cybersecurity fundamentals [24] [25], though enforcement and standardization remain inconsistent. Unlike cybersecurity education frameworks, AI education lacks a standardized set of knowledge units linking competencies and job functions. This gap becomes increasingly problematic as workforce frameworks have begun establishing AI-related workforce requirements. The U.S. Department of Defense (DoD) Cybersecurity Workforce Framework (DCWF) outlined 54 work roles, of which 11 fall within the Data/AI category [26]. DCWF provides an opportunity to build upon and complement the NICE Framework for cybersecurity and AI work roles' TKSs, yet education programs lack structured guidance for developing AI-related curriculum.

2.4 Gaps and Future Directions for AI and Cybersecurity Standards

Knowledge Units (KUs) represent discrete curricular building blocks tied to defined learning outcomes. KU-based curricula enhance transparency and comparability across programs. These require periodic updates and adoption. Developing and deploying validated KUs and validation programs for cybersecurity and AI are a priority for academia and a strategic national imperative. Workforce readiness depends on embedding these competencies across disciplines, supported by evidence-based curricular standards.

The lack of AI-specific KUs and specifically, those related to cybersecurity, provides an opportunity to develop these KUs mapped to industry needs and NICE Framework and DCWF work roles. AI knowledge units could align with the existing frameworks previously outlined or mapping to ABET guidelines that emphasize ethics, computing foundations, and interdisciplinary understanding [27]. Despite this, curriculum designers must contend with evolving technologies, cybersecurity threats, AI tools, limited faculty expertise, and institutional bureaucracies. Standards development requires collaboration across academia, accrediting bodies, and industry to ensure relevance, quality, and flexibility.

Beyond technical skills, a competent workforce requires adaptability, ethical reasoning, and systems thinking, which are considered essential attributes for navigating complex, high-stakes environments.

Additionally, integrating cognitive thinking skills and technical-centric and human-centric skills [28] leads to programs that empower cybersecurity professionals.

3 Methodology

The rapid pace of development for the SecureAI and AICyber KUs represents a significant departure from traditional curriculum design timelines. Driven by the urgency of integrating AI competencies into cybersecurity education, the entire KU development cycle—from initial drafting to live release—was accomplished in under five months. This accelerated timeline was made possible through the combined use of AI-assisted drafting tools, coordinated national workshops, and a highly engaged academic community. The swift iterations of the "Straw Man" and the current "Stone Man" versions illustrate a model of agile curricular guidelines responsive to technological change and workforce demands. The development of SecureAI and AICyber KUs followed a structured, iterative approach led by a consortium of twelve subject matter experts (SMEs) from nine NSA-designated Centers of Academic Excellence (CAE) institutions. These experts included representatives with prior experience developing academic KUs, professional frameworks, and standards.

Initial drafts began with six "Straw Man" versions and culminated in a final "Stone Man" draft, incorporating feedback from workshops, webinars, and federal stakeholders. In addition to human input, AI assistants were also employed to assist with the formulation of learning outcomes and KU descriptions, reflecting a novel and efficient use of generative AI in curriculum guideline development [29]. The final Stone Man version incorporated input from over 200 individuals, including educators, practitioners, federal partners, and academic stakeholders engaged throughout the development process.

Each KU consists of a title, description, learning outcomes, topics, and notes. Learning outcomes are grounded in Bloom's Taxonomy and designed to support diverse pedagogical models, including experiential and lab-based learning. The KUs were structured to allow alignment across varying academic levels and disciplines, supporting modular and stackable credentials.

The KU development was guided by principles of national scalability, cross-disciplinary relevance, and responsiveness to technological trends. Feedback loops ensured transparency and refinement through broad community input, and validation workshops ensured the final KUs met both academic rigor and workforce relevance.

4 Programs of Study (PoS)

The "StoneMan" [30] document contains detailed information on the Programs of Study (PoS) and KUs. CyberAI programs were broken down into two distinct PoS defined below and outlined in the Thought Model (Figure 1):

- Security of AI (SecureAI): Securing AI systems and infrastructure throughout their lifecycle.
- AI for Cybersecurity (AICyber): Leveraging AI to support traditional cybersecurity.

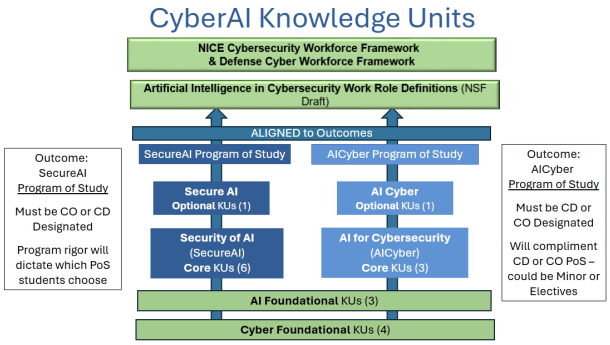

Figure 1: CyberAI Curriculum Guideline thought model. The "CD" and "CO" refer to the NSA CAE designations.

This initiative defined a KU as a thematic grouping that encompasses multiple, related KU outcomes and learning topics [30]. A KU outcome is a specific assessment of a concept associated with a particular KU [30]. Each KU was developed based on a specified structure, including the following:

- Name: Used to identify a KU followed by a three-letter key used for indexing in data structures [30].
- Description: Short narrative description of the scope and contents of the KU with the intent to provide students with [basic/intermediate/advanced] awareness of [details] [30].
- Outcomes: Description of student-based outcomes associated with the KU [30].
- KU Topics: A list of elements in the KU listed in an appropriate hierarchy of detail [30].

The KUs for each PoS are broken down into Cyber Foundational, AI Foundational, Core, and Optional KUs (Figure 2). Cyber Foundational and AI Foundational are consistent across Programs of Study. Cyber Foundational KUs include Cybersecurity Fundamentals (CSF), IT Systems Components (ISC), Basic Scripting and Programming (BSP), and Math Fundamentals (MAF). AI Foundational KUs include AI Governance, Laws, and Ethics (AIG); AI Fundamentals (AIF); and Machine Learning Fundamentals (MLF). Core and Optional KUs align with the overarching requirements for each PoS. SecureAI Core KUs include Computer Science Foundations (COF), Advanced Math for AI (AVM), Securing the AI Lifecycle (AIL), Machine Learning Algorithms (MLA), Deep Learning (DPL), Adversarial Learning (ADL), and Optional KUs include Model Selection, Evaluation, and Specification (MES) and Risk Management of AI (AIR). AICyber Core KUs include Basic Networking (BNW), Network Defense (NDF), and AI for Security Assessment (AIS), Optional KUs include Defensive Applications of AI (DFA), and Offensive Applications of AI (OFA).

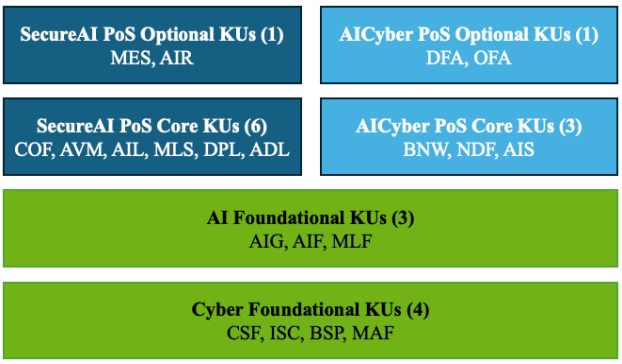

Figure 2: CyberAI PoS KU Breakdown and Alignment

5 Validation Framework and Pilot Implementation

Validation of the SecureAI and AICyber PoS followed National Centers of Academic Excellence in Cybersecurity (NCAE-C) protocols adapted for AI integration. As outlined in the 2024 CyberAI PoS Validation Requirements document [31], programs seeking validation must demonstrate alignment with foundational, core, and optional KUs, submit detailed curriculum maps, provide course syllabi with lab exercises, and document program-level learning outcomes tied to NICE/DCWF work roles. Applying institutions must maintain one of the NCAE-C designations: Cyber Operations (CAE-CO) and/or Cyber Defense (CAE-CD).

Pilot implementations took place across 16 institutions (with most four-year colleges) beginning in March 2025. Four institutions applied for SecureAI and 12 institutions for AICyber. These pilots were preceded by peer reviewer selection, faculty mentor training, and intensive workshops. Feedback from student artifacts, faculty surveys, and validation rubrics informed final adjustments to both the KU documents and validation tools.

Institutions applied using a formal adjudication rubric and were required to submit KU alignment evidence, student work samples, and proof of continuous improvement cycles. A major innovation was the use of digital equivalency metrics for courses with multiple sections, allowing for uniform validation while accommodating institutional diversity.

The pilot phase concluded in June 2025 and the first validated programs will be officially recognized by October 2025. These PoS serve as exemplars for future implementations across the CAE-CD and CAE-CO communities.

6 Future Work and Conclusions

The integration of AI into cybersecurity education presents numerous challenges, many of which emerged during the development and pilot of the SecureAI and AICyber Programs of Study. Foremost among these is the rapid evolution of AI tools and techniques, which necessitates continual curriculum updates. Unlike foundational math and computer science topics, cybersecurity topics, and AI developments often outpace academic publishing cycles, requiring institutions to adopt more agile content review and delivery models.

Another challenge is the interdisciplinary nature of AI. Ethical, legal, and societal implications of AI must be embedded within technical courses. This task requires collaboration between computer science, engineering, policy, and humanities faculty. The Knowledge Units, specifically AI Governance, Laws, and Ethics (AIG), addresses these issues, but institutions must go beyond checkbox compliance to foster meaningful student engagement with these topics.

Scalability also remains a critical concern. Institutions with limited resources may struggle to offer AI-focused lab experiences, especially those involving adversarial testing or deep learning frameworks. Centralized repositories shared virtual environments, and national consortia like the CAE Community of Practice (CoP) can alleviate some of these barriers. Additionally, faculty members with expertise in cybersecurity and AI are limited, further limiting the scalability of these programs.

Despite these obstacles, the SecureAI and AICyber KU models offer a promising template for modernizing cybersecurity and AI education. By leveraging national frameworks and aligning with national priorities, these PoS support institutional innovation while maintaining rigorous validation standards. The integration of AI assistants during KU development also opens a new frontier for AI-in-the-loop curriculum design, reducing faculty burden while enhancing quality assurance [29].

In conclusion, the development and validation of AI-integrated KUs represent a transformative step in cybersecurity and AI education. These frameworks ensure that graduates possess both foundational security knowledge and fluency in AI tools and ethics. As technology continues to evolve, programs that embed adaptability, interdisciplinarity, and continuous improvement into their core will be best positioned to prepare the next generation of cybersecurity professionals.

Acknowledgements

This project is partially funded by NSF through the CyberCorps program DGE#1663184 at Towson University. We acknowledge all the faculty listed in the StoneMan draft for their contributions. This work could not be completed without the support of the DOD CAEO office and the NSA NCAE-C program management office.

References

<bib id="bib1"><number>[1]</number>Cagatay Catal, Alper Ozcan, Emrah Donmez, and Ahmet Kasil. 2022. Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education and Information Techcnologies.* 1809-1831. DOI: https://doi.org/10.1007/s10639-022-11261-8.</bib>
<bib id="bib2"><number>[2]</number>Saadia Zahidi. 2023. Future of Jobs Report 2023. *World Economic Forum.* https://www.weforum.org/publications/the-future-of-jobs-report-2023/.</bib>
<bib id="bib3"><number>[3]</number>U.S. Bureau of Labor and Statistics. 2025. Information Security Analysts. *Occupational Outlook Handbook.* https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.</bib>
<bib id="bib4"><number>[4]</number>ISC2. 2024. Global Cybersecurity Workforce Prepares for an AI-Driven World. *ISC2 Cybersecurity Workforce Study*. https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study.</bib>
<bib id="bib5"><number>[5]</number>Cyberseek. 2025. Cybersecurity Supply/Demand Heat Map. *Cyberseek*. https://www.cyberseek.org/heatmap.html.</bib>
<bib id="bib6"><number>[6]</number>ISACA. 2024. State of Cybersecurity 2024 Global Update on Workforce Efforts, Resources, and Cyberoperations. *ISACA.* https://www.isaca.org/resources/reports/state-of-cybersecurity-2024.</bib>
<bib id="bib7"><number>[7]</number>ISACA. 2025. 89% of Digital Trust Pros Say Increased AI Skills and Knowledge Needed to Retain Job or Advance Their Career Over Next Two Years. *ISACA*. https://www.isaca.org/about-us/newsroom/press-releases/2025/digital-trust-pros-say-increased-ai-skills-and-knowledge-needed-to-advance-their-career.</bib>
<bib id="bib8"><number>[8]</number>NIST. 2023. Artificial Intelligence Risk Management Framework (AI RMF 1.0). *National Institute of Standards and Technology U.S. Department of Commerce*. DOI: https://doi.org/10.6028/NIST.AI.100-1.</bib>
<bib id="bib9"><number>[9]</number>Ruti Gafni and Yair Levy. 2024. The role of artificial intelligence (AI) in improving technical and managerial cybersecurity tasks' efficiency. *Information and Computer Security*. 711–728. DOI: https://doi.org/10.1108/ICS-04-2024-0102</bib>
<bib id="bib10"><number>[10]</number>Rodney Petersen, Danielle Santos, Matthew Smith, Karen Wetzel, and Greg Witte. 2020. NIST SP 800-181r1 Workforce Framework for Cybersecurity (NICE Framework). *National Institute of Standards and Technology U.S. Department of Commerce*. DOI: https://doi.org/10.6028/NIST.SP.800-181r1.</bib>
<bib id="bib11"><number>[11]</number>NICE Workforce Framework for Cybersecurity. *National Initiative for Cybersecurity Careers and Study (NICCS).* https://niccs.cisa.gov/tools/nice-framework.</bib>

<bib id="bib12"><number>[12]</number>Awais Rashid, Howard Chivers, Emil Lupu, Andrew Martin, and Steve Schneider. 2021. The Cybersecurity Body of Knowledge. *The national Cyber Security Centre*. https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf.</bib>
<bib id="bib13"><number>[13]</number>Diana Burley, Matt Bishop, Scott Buck, Joseph Ekstrom, Lynn Futcher, David Gibson, Elizabeth Hawthorne, Siddharth Kaza, Yair Levy, Herbert Mattrod, and Allen Parrish. 2017. Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. *Association for Computing Machinery*. https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf.</bib>
<bib id="bib14"><number>[14]</number>Paresh Rathod. 2022. European Cybersecurity Education and Professional Training: Minimum Reference Curriculum. *European Cyber Security Organisation*. https://ecs-org.eu/ecso-uploads/2022/12/2022_SWG5.2_Minimum_Reference_Curriculum_final_v3.0.pdf.</bib>
<bib id="bib15"><number>[15]</number>Zaina Dkaidek and Awais Rashid. 2024. Bridging the Cybersecurity Skills Gap: Knowledge Framework Comparative Study. *IEEE Security and Privacy*. 88-95. DOI: https://doi.org/10.1109/MSEC.2024.3428892.</bib>
<bib id="bib16"><number>[16]</number>Gelareh Towhidi and Jeannie Pridmore. 2023. Aligning Cybersecurity in Higher Education with Industry Needs. *Journal of Information Systems Education.* 70-83. https://jise.org/Volume34/n1/JISE2023v34n1pp70-83.html.</bib>
<bib id="bib17"><number>[17]</number>Madhav Mukherjee, Ngoc Thuy Le, Yang-Wai Chow, and Willy Susilo. 2024. Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. *MDPI Information*. 117-140. DOI: https://doi.org/10.3390/info15020117.</bib>
<bib id="bib18"><number>[18]</number>Muhusina Ismail, Nisha Madathil, Meera Alalawi, Saed Alrabaee, Mohammad Bataineh, Suhib Melhem, and Djedjiga Mouheb. 2024. Cybersecurity activities for education and curriculum design: A survey. *Computers in Human Behavior*. DOI: https://doi.org/10.1016/j.chbr.2024.100501.</bib>
<bib id="bib19"><number>[19]</number>Izzat Alsmadi. 2018. Cybersecurity Education Based on the NICE Framework: Issues and Challenges. *ISACA*. https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/cybersecurity-education-based-on-the-nice-framework-issues-and-challenges.</bib>
<bib id="bib20"><number>[20]</number>Milla Surjadi. 2024. Colleges Race to Ready Students for the AI Workplace. *The Wall Street Journal*. https://www.wsj.com/us-news/education/colleges-race-to-ready-students-for-the-ai-workplace-cc936e5b?reflink=desktopwebshare_permalink.</bib>
<bib id="bib21"><number>[21]</number>Jane Southworth, Kati Migliaccio, Joe Glover, Ja'Net Glover, David Reed, Christopher McCarty, Joel Brendemuhl, and Aaron Thomas. 2023. Developing a model for AI Across the Curriculum: Transforming the higher education landscape via innovation in AI literacy. *Computer and Education: Artificial Intelligence*. DOI: https://doi.org/10.1016/j.caeai.2023.100127.</bib>
<bib id="bib22"><number>[22]</number>Yoshija Walter. 2024. Embracing the future of Artificial Intelligence in the classroom: the relevance of AI literacy, prompt engineering, and critical thinking in modern education. *International Journal of Educational Technology in Higher Education*. DOI: https://doi.org/10.1186/s41239-024-00448-3.</bib>
<bib id="bib23"><number>[23]</number>Miguel Cardona and Roberto Rodriguez. 2025. Navigating Artificial Intelligence in Postsecondary Education: Building Capacity for the Road Ahead. *Office of Educational Technology*. https://files.eric.ed.gov/fulltext/ED670768.pdf.</bib>
<bib id="bib24"><number>[24]</number>2025. Certificate Program in Applied Generative AI. *Johns Hopkins Whiting School of Engineering*. https://online.lifelonglearning.jhu.edu/jhu-certificate-program-applied-generative-ai.</bib>
<bib id="bib25"><number>[25]</number>2025. Applied AI and Data Science Program. *MIT Professional Education*. https://professional-education-gl.mit.edu/mit-applied-data-science-course.</bib>
<bib id="bib26"><number>[26]</number>2025. DoD Cyber Workforce Framework. *DoD Cyber Exchange Public*. https://public.cyber.mil/wf-element-sub/ai-data/.</bib>
<bib id="bib27"><number>[27]</number>2025. Criteria for Accrediting Computing Programs, 2025-2026. *ABET*. https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2025-2026/.</bib>
<bib id="bib28"><number>[28]</number>Nageswaree Ramsoonder, Selvamanee Kinnoo, Anna Griffin, Craig Valli, and Nicola Johnson. 2021. Optimizing Cyber Security Education: Implementation of Bloom's Taxonomy for future Cyber Security workforce. *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*. DOI: http://dx.doi.org/10.1109/CSCI51800.2020.00023.</bib>
<bib id="bib29"><number>[29]</number>Paige Zaleppa, Siddharth Kaza, Blair Taylor, and Md Sajidul Islam. 2024. Using AI Assistants in the Creation of an Academic Program of Study (PoS) in CyberAI. *Proceedings of the 28th Colloquium for Information Systems Security Education (CISSE)*. DOI: https://doi.org/10.53735/cisse.v12i1.</bib>
<bib id="bib30"><number>[30]</number>Shankar Banik, Eman El-Sheikh, Paige Flores, Seth Hamman, Siddharth Kaza, Yair Levy, Vincent Nestler, Md Sajid, Sagar Samtani, Patrick Tague, Blair Taylor, Paul Wagner. 2024. Cyber AI Programs Stoneman v1. *Department of Defense Cyber Exchange*. https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cyber_ai_kus_stoneman.pdf.</bib>
<bib id="bib31"><number>[31]</number>CyberAI Working Group. 2024. Program Validation Requirements and Application Process for CyberAI Programs of Study (CyberAI). *National Centers of Academic Excellence in Cybersecurity*. https://public.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae_pos-cyberai.pdf.</bib>