Scientific Research Publishing

Journal of Intelligent Learning Systems and Applications, 2025, 17(2), 45-67
https://www.scirp.org/journal/jilsa
ISSN Online: 2150-8410
ISSN Print: 2150-8402

Integrating AI in Cybersecurity Higher Education: A Path to Workforce Readiness

Maryam Roshanaei, Mark Gregory Jachura

Pennsylvania State University, Abington, Abington, USA
Email: m.roshanaei@psu.edu

How to cite this paper: Roshanaei, M. and Jachura, M.G. (2025) Integrating AI in Cybersecurity Higher Education: A Path to Workforce Readiness. *Journal of Intelligent Learning Systems and Applications*, **17**, 45-67.
https://doi.org/10.4236/jilsa.2025.172005

Received: February 6, 2025
Accepted: March 28, 2025
Published: March 31, 2025

Abstract

The rapid evolution of cyber threats has intensified the need for advanced educational frameworks that equip future professionals with the skills to tackle emerging challenges. Artificial Intelligence (AI) has become a transformative force in cybersecurity, offering enhanced threat detection, automated response mechanisms, and predictive analytics. However, integrating AI into cybersecurity higher education remains a challenge due to curriculum gaps, faculty expertise limitations, and resource constraints. This paper proposes a multidimensional framework to incorporate AI into cybersecurity education through hands-on training, faculty development, and curriculum restructuring. By leveraging AI-driven methodologies and industry collaborations, the framework aims to bridge the skills gap and prepare students for real-world cybersecurity challenges. The study highlights key strategies for improving workforce readiness and ensuring that graduates possess the competencies required to navigate the dynamic threat landscape effectively.

Keywords

Cybersecurity, Artificial Intelligence, Higher Education, Workforce Development

1. Introduction

The rapid evolution of technology has revolutionized industries, reshaping the global landscape of commerce, communication, and critical infrastructure [1]. However, this technological progress has also introduced significant vulnerabilities, as cybersecurity threats continue to evolve in scale, sophistication, and frequency. From ransomware attacks crippling major institutions to large-scale data breaches compromising sensitive information, the threat landscape is increasingly dynamic and challenging [2]. Amid these challenges, artificial intelligence (AI)

has emerged as a transformative force in the field of cybersecurity. Its ability to process vast amounts of data in real-time, identify anomalies, and predict potential threats has positioned AI as a critical tool in detecting, mitigating, and even preventing cyberattacks [3]. Organizations across various sectors are leveraging AI-driven tools for tasks ranging from threat intelligence to automated incident response, highlighting its indispensable role in safeguarding digital ecosystems [4].

Despite these advancements, higher education institutions often struggle to keep pace with the rapid adoption of AI in the cybersecurity domain. Many programs remain rooted in traditional methodologies, leaving graduates underprepared for the demands of a rapidly changing industry. The lack of AI-centric curricula represents a missed opportunity to equip students with the skills and knowledge necessary to address modern cybersecurity challenges. This importance emphasizes the critical role of integrating AI into cybersecurity education to address the growing skills gap and prepare a workforce capable of navigating future challenges. By aligning educational strategies with emerging industry trends and technological advancements, it highlights how AI-driven programs can foster innovation, enhance resilience, and equip professionals with the adaptability needed to combat the evolving landscape of digital threats [5].

2. The Need for AI in Cybersecurity Higher Education

Traditional cybersecurity education has long emphasized foundational areas such as network security, cryptography, and risk management [6]. While these disciplines remain essential, they are increasingly inadequate in addressing the sophisticated and evolving nature of modern cyber threats. Emerging challenges, such as AI-generated phishing campaigns and deepfake attacks, exploit advanced technologies that traditional methods are ill-equipped to counter [7].

This gap underscores the critical need to incorporate AI into cybersecurity education. AI integration offers transformative benefits that address the limitations of conventional approaches [8]. **Table 1** highlights the key benefits of integrating AI into cybersecurity education, showcasing its ability to enhance threat detection, enable proactive defense mechanisms, and support skill development in advanced technologies [9].

Table 1. Key benefits of integrating AI into cybersecurity education.

Key Benefit	Description
Enhanced Threat Detection	Machine learning algorithms analyze vast datasets to identify anomalies and potential threats with speed and precision.
Proactive Defense Mechanisms	AI models predict potential attack vectors, enabling preemptive measures to mitigate risks before they occur.
Skill Development	Expertise in AI-driven tools, such as natural language processing for phishing detection and deep learning models for malware analysis.

Incorporating AI into cybersecurity education is no longer optional—it is an imperative for preparing the next generation of professionals to combat the increasingly complex and technology-driven threat landscape. By equipping students with the knowledge and tools to harness AI, educational institutions can bridge the skills gap and empower future professionals to anticipate, prevent, and respond to advanced cyber threats [10]. While the integration of AI into cybersecurity education offers significant benefits, several challenges hinder its widespread adoption. Institutions must navigate these barriers to effectively prepare students for the demands of the modern cybersecurity landscape.

3. Resource Constraints

AI-driven cybersecurity programs often require significant investments in infrastructure, tools, and software. According to a report by Gartner[1], global spending on AI is projected to reach $154 billion by 2025, with cybersecurity accounting for a substantial portion [11]. High-performance computing resources, specialized software for machine learning, and access to real-world datasets are essential for a comprehensive learning experience. However, many institutions, particularly smaller universities, face constrained budgets, making it difficult to acquire and maintain these resources. Additionally, continuous updates are necessary to keep pace with the rapid evolution of AI and cybersecurity technologies, further straining financial resources. According to Gartner's press release on January 21, 2025, worldwide IT spending is projected to reach $5.3 trillion in 2025, representing a 9.8% increase from 2024. This growth is driven by investments in cloud computing, artificial intelligence, and cybersecurity. Table 2 outlines the forecasted IT spending across key segments in 2025, highlighting an overall 9.8% year-over-year growth driven by advancements in software, IT services, and communications technology [12].

Table 2. Projected worldwide IT spending for 2025.

Segment	Spending (USD)	Year-over-Year Growth
Data Center Systems	$250 billion	5%
Software	$1.2 trillion	12%
Devices	$800 billion	7%
IT Services	$1.5 trillion	10%
Communications	$1.55 trillion	8%

4. Skill Gaps Among Educators

A critical bottleneck in implementing AI-centric cybersecurity programs lies in the expertise of faculty members. A 2024 study by Burning Glass Technologies[2]

[1]https://www.gartner.com/en.
[2]https://www.burningglassinstitute.org/.

found that job postings requiring both AI and cybersecurity expertise have grown by over 40% annually, underscoring the increasing demand for such skills [13]. The Center on Reinventing Public Education (CRPE)[3] at Arizona State University[4] surveyed and interviewed over 500 U.S. education school leaders to explore the integration of AI into teacher training programs. The research aimed to uncover how faculty and preservice teachers interact with AI, their views on the technology's long-term influence on education, and the steps institutions are taking to incorporate AI into their curricula and coursework. Although the response rate was moderate at 14%, the surveyed institutions train hundreds of future teachers annually, providing valuable initial insights into teacher preparation in the era of generative AI. The findings reveal that most institutions are struggling to keep up with the rapid technological advancements transforming classrooms across the country [14].

Only 10% of surveyed education school leaders reported that their faculty feel confident using AI, with most faculty not incorporating it into their teaching. Additionally, over half of the respondents noted that faculty lack confidence in integrating AI tools and resources into their instructional practices. **Table 3** illustrates the varying levels of confidence among faculty regarding the integration of AI tools and resources into their teaching practices [15].

Table 3. Faculty confidence in integrating AI tools into teaching.

Statement	Response	Percentage of Respondents
Faculty feel very confident in effectively integrating AI tools and resources into teaching	Strongly Agree	2%
Faculty feel confident in integrating AI tools into teaching	Agree	8%
Faculty have neutral confidence regarding AI integration	Neutral	20%
Faculty feel not confident in integrating AI tools into teaching	Disagree	40%
Faculty feel very unconfident about integrating AI tools into teaching	Strongly Disagree	30%

Inside Higher Ed's 2024 Survey of Campus Chief Technology/Information Officers, conducted by Hanover Research[5], highlights mixed perspectives on the integration of artificial intelligence (AI) in higher education [16]. While many technology leaders see potential in AI to enhance institutional capabilities, there is significant concern about its risks, particularly regarding academic integrity. The

[3]https://crpe.org/.
[4]https://www.asu.edu/.
[5]https://www.hanoverresearch.com/.

survey also indicates that institutions tend to focus on specific AI applications, such as chatbots and virtual assistants, rather than adopting comprehensive AI strategies. Additionally, prioritization of AI investment remains low across many institutions. Table 4 provides a summary of AI preparedness among higher education institutions, highlighting low overall confidence in readiness, moderate adoption of AI applications, significant concerns about academic integrity, low prioritization of AI investments, and mixed enthusiasm regarding AI's potential to enhance institutional capabilities [17].

Table 4. AI preparedness in higher education institutions.

Category	Description	Findings
Overall AI Preparedness	Confidence in readiness to handle AI integration	Low confidence
Focus on AI Applications	Use of specific tools like chatbots and virtual assistants	Moderate adoption
Academic Integrity Concerns	Perceived risks of AI in education	Significant concern
AI Investment Prioritization	Institutions prioritizing AI-related investments	Low priority
Potential for Institutional Enhancement	Enthusiasm about AI improving institutional capabilities	Mixed enthusiasm

A significant challenge in integrating AI into cybersecurity education is the lack of hands-on experience among faculty members with cutting-edge AI tools, such as machine learning frameworks and advanced threat detection systems. A 2024 survey conducted by Inside Higher Ed[6] revealed that only 10% of education faculty feel confident teaching AI concepts effectively [18]. This gap in proficiency includes limited familiarity with tools like TensorFlow[7], PyTorch[8], and specialized cybersecurity platforms such as Splunk[9] or IBM QRadar[10]. Without practical experience, faculty struggle to design robust curricula and deliver instruction that reflects the current needs of the field [19]. The rapid pace of advancements in AI and cybersecurity further exacerbates this issue. Faculty members who lack exposure to evolving technologies, such as AI-based malware detection or automated threat intelligence systems, are often unable to keep their course content relevant. This disconnect negatively impacts students' preparedness for the workforce. For instance, a Deloitte[11] report found that 64% of cybersecurity roles now require

[6]https://www.insidehighered.com/.
[7]https://www.tensorflow.org/.
[8]https://pytorch.org/.
[9]https://www.splunk.com/.
[10]https://www.ibm.com/qradar.
[11]https://www2.deloitte.com/us/en.html.

expertise in AI-driven tools, yet many graduates fall short of these expectations due to insufficient exposure to practical, AI-focused education [20].

The lack of faculty expertise also limits students' ability to innovate. When educators are unable to mentor students effectively in developing custom machine learning models or designing novel AI-based threat mitigation strategies, creativity and exploration in the classroom are stifled. This limitation has broader implications, as it contributes to the ongoing cybersecurity talent shortage. According to Cybersecurity Ventures[12], there will be 3.5 million unfilled cybersecurity jobs globally by 2025, many of which will require AI expertise. Bridging this gap in faculty knowledge is therefore critical to producing graduates who can meet industry demands [21].

5. Curriculum Design

A 2023 survey by the Ponemon Institute[13] highlights a significant gap in the preparedness of university cybersecurity programs. According to the survey, 68% of cybersecurity professionals believe that current educational programs are not adequately equipping graduates to handle real-world challenges, particularly in the context of AI-driven threat detection and response. This statistic underscores a critical disconnect between academic training and industry requirements [22]. One of the key areas of concern is the lack of hands-on experience with advanced AI technologies. Many university programs still focus on traditional cybersecurity methods, often neglecting the practical application of AI-based tools such as machine learning algorithms for anomaly detection or automated threat intelligence systems. As a result, graduates enter the workforce with theoretical knowledge but limited experience in using the tools and technologies required to combat sophisticated cyber threats [23]. The findings further emphasize the increasing reliance on AI in cybersecurity. AI is revolutionizing the field by enabling faster and more accurate identification of threats, automating repetitive tasks, and improving response times. However, without proper training, new professionals may struggle to leverage these technologies effectively, leading to a skills gap that could hinder organizational efforts to maintain robust cybersecurity defenses [24]. To address this issue, universities must revamp their curricula to include practical training on AI-driven cybersecurity tools. Partnerships with industry can play a pivotal role in this transformation by providing students and faculty with access to the latest technologies and real-world use cases. Additionally, faculty development programs focused on AI in cybersecurity can help bridge the expertise gap, ensuring that educators can deliver relevant and up-to-date instruction [25]. The research also suggests that fostering innovation in cybersecurity education is essential to preparing students for emerging challenges. Encouraging project-based learning and internships that emphasize AI applications can inspire students to explore creative solutions and develop critical problem-solving skills. By aligning aca-

[12]https://cybersecurityventures.com/.
[13]https://www.ponemon.org/.

demic programs with industry needs, universities can not only enhance graduate employability but also contribute to strengthening the global cybersecurity landscape, as shown in Figure 1 [26].

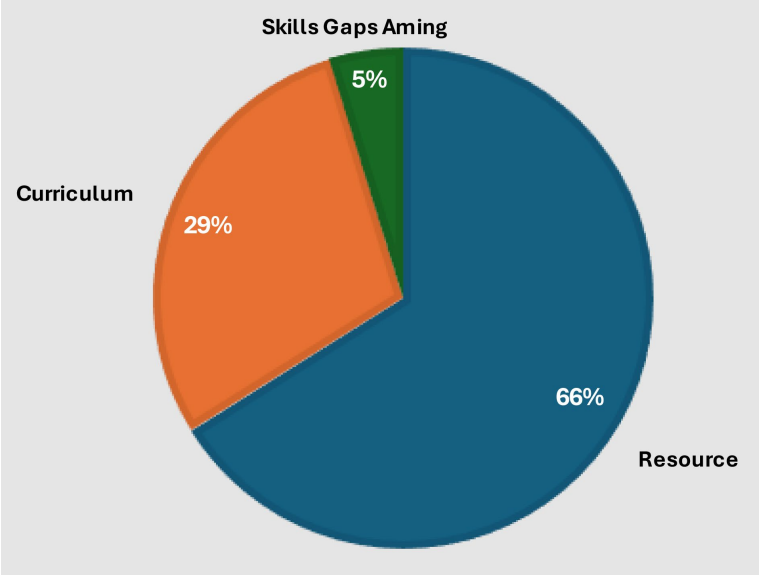

Figure 1. Challenges in AI integration for cybersecurity education.

6. Existing Methodologies and Examples of AI Integration in Cybersecurity Education

Carnegie Mellon University[14] (CMU) is renowned for its innovative methodologies in integrating AI and cybersecurity into its curriculum. The university adopts a multidisciplinary approach, combining theoretical instruction, hands-on practice, and research opportunities to equip students with both foundational knowledge and advanced technical expertise. As part of its methodology, CMU offers a range of core and specialized courses. Foundational courses such as Introduction to Machine Learning and Foundations of Cybersecurity provide students with the basics of AI and cybersecurity, ensuring a strong knowledge base [27]. Advanced modules like AI for Cybersecurity focus on applying machine learning models to real-world challenges, including threat detection, incident response, and adversarial machine learning. Additionally, students are engaged in research and capstone projects that address pressing cybersecurity issues. For example, students have worked on developing machine learning algorithms to identify zero-day attacks and automating malware analysis, bridging the gap between theory and practical application [28].

One notable project at CMU involved developing an AI-driven anomaly detection system for network traffic. The primary objective of this project was to reduce false-positive rates in identifying potential cyberattacks. Students utilized publicly available datasets such as CICIDS2017 [29] and UNSW-NB15 [30], which contain

[14]https://www.cmu.edu/.

labeled network traffic data for both normal and malicious activities. Machine learning models, including Random Forest, Support Vector Machines (SVM), and Neural Networks, were trained to distinguish between normal and anomalous behaviors. The methodology also involved preprocessing data through feature selection, normalization, and dimensionality reduction using Principal Component Analysis (PCA). As shown in Table 5, it reduced false-positive rates from 15% to 4%, a significant improvement over traditional threshold-based detection system. The anomaly detection system achieved an overall accuracy of 92%, surpassing the industry benchmark of 85%. Detailed model performance metrics included a precision of 91%, recall of 93%, and an F1-Score of 92%. To validate the system's effectiveness, students relied on the CICIDS2017 dataset, which contains over 3 million records of network traffic data, including 2.3 million normal instances and 700,000 malicious ones across 14 attack scenarios (e.g., DoS, brute force, and botnets). The models were tested using a 5-fold cross-validation process to ensure generalizability, with Random Forest outperforming other algorithms by achieving a detection rate of 93% for malicious traffic and a false alarm rate of only 3.5% [31].

Table 5. Performance evaluation of an AI-driven anomaly detection system.

Metric	Outcome
False-Positive Rate Reduction	Decreased from 15% to 4%, significantly improving detection accuracy.
Anomaly Detection Accuracy	Achieved 92%, surpassing the industry benchmark of 85%.
Model Performance Metrics	Precision: 91%, Recall: 93%, F1-Score: 92%.
Dataset Used	CICIDS2017 (3 million records: 2.3M normal, 700K malicious).
Attack Scenarios Covered	14 types (e.g., DoS, brute force, botnets).
Validation Method	5-fold cross-validation to ensure generalizability.
Best Performing Model	Random Forest with a 93% detection rate for malicious traffic.
False Alarm Rate	3.5%, indicating strong model reliability.

Further testing in simulated environments revealed a 30% improvement in response time, enabling faster containment of threats. These outcomes demonstrated the real-world applicability of the methodology, solidifying CMU's position as a leader in AI-driven cybersecurity education. The project not only provided a cutting-edge solution but also equipped students with the skills and experience needed to address complex cybersecurity challenges in professional envi-

ronments [32].

Stanford University[15] integrates AI and cybersecurity into its interdisciplinary programs, leveraging expertise from computer science, law, and ethics to provide students with a holistic understanding of the field. This approach equips students with technical proficiency while addressing broader issues such as ethical AI deployment, bias in algorithms, and data privacy. As part of its methodology, Stanford offers interdisciplinary courses like AI, Ethics, and Cybersecurity, which blend technical knowledge with discussions on the societal implications of AI. These courses enable students to critically assess the risks and challenges associated with AI applications in cybersecurity. In addition to theoretical instruction, hands-on training plays a crucial role in Stanford's program. Students gain experience using tools such as TensorFlow and Splunk to build and deploy AI-powered threat intelligence systems. The university also emphasizes collaboration with industry leaders like Google and Microsoft, providing students with access to real-world datasets and proprietary AI tools, enhancing their practical knowledge. A standout project within Stanford's program involved developing a machine learning model for phishing email detection. The project, conducted in collaboration with industry partners, aimed to enhance the accuracy and efficiency of phishing detection systems. Students worked with a combined dataset of over 200,000 phishing and legitimate emails, sourced from the Enron Email Dataset and the Phishing Email Corpus [33].

The project employed advanced Natural Language Processing (NLP) techniques such as tokenization, sentiment analysis, and bag-of-words to extract linguistic features from email content [34]. Students applied machine learning models including Logistic Regression, Gradient Boosting, and Transformer-based models like BERT. The inclusion of adversarial training ensured the model's robustness against sophisticated phishing attacks designed to evade traditional filters [35]. The project outcomes were remarkable. The model achieved a detection accuracy of 95%, surpassing the industry benchmark of 87%. Its robustness was demonstrated by a success rate of 89% in detecting zero-day phishing emails, showcasing its adaptability to novel phishing patterns. Additionally, the system reduced manual email review efforts by 60%, significantly freeing up resources for other cybersecurity tasks. This study utilized emails from the Enron Email Dataset and the Phishing Email Corpus for model training and testing [36].

Data preprocessing involved removing duplicates, anonymizing sensitive information, and extracting linguistic features such as word frequency and domain reputation. NLP techniques, including TF-IDF (Term Frequency-Inverse Document Frequency) and the advanced deep learning model BERT, were implemented, with BERT achieving the highest accuracy compared to Logistic Regression and Random Forest. Additionally, adversarial testing demonstrated that phishing emails specifically designed to evade traditional filters were successfully identified in most cases [37]. The project's success was validated through a part-

[15]https://www.stanford.edu/.

nership with Google, where the model was integrated into the Gmail spam filter for pilot testing. The results showed a 25% reduction in phishing-related compromises, underscoring the model's practical applicability and scalability. This success led to the widespread adoption of the system [38]. Stanford's phishing detection project exemplifies the power of NLP in addressing cybersecurity challenges [39]. By combining rigorous academic instruction, hands-on training, and industry collaboration, the university has demonstrated how cutting-edge AI technologies can effectively tackle real-world problems [40]. The outcomes of this project not only highlight the practical significance of AI-powered cybersecurity tools but also reinforce the importance of interdisciplinary education in preparing students for the complexities of modern cybersecurity threats [41].

The University of New South Wales[16] (UNSW) [42] adopts a hands-on, practical approach to integrating AI into its cybersecurity programs, emphasizing real-world applications and collaboration with industry partners [43]. By leveraging AI-equipped labs, capstone projects, and industry mentorship, UNSW ensures students gain technical expertise and practical experience needed to tackle complex cybersecurity challenges [44]. Students have access to state-of-the-art cybersecurity labs, where they use simulation tools to detect and mitigate cyberattacks. These labs provide an environment for experimenting with advanced AI tools and methodologies, bridging the gap between theoretical learning and application [45].

Capstone projects are a key feature of the program, requiring students to develop and implement AI models to address real-world cybersecurity problems. Additionally, UNSW pairs students with industry mentors who guide them in applying AI techniques to solve pressing challenges, offering valuable insights into current industry practices [46]. One standout project from UNSW involved the development of an AI-powered penetration testing framework designed to automate the identification of vulnerabilities in web applications [47]. The project aimed to enhance the efficiency and accuracy of penetration testing by leveraging AI [48]. Students used datasets such as the OWASP Vulnerable Web Applications Dataset (VWAD) and the CVE Database, which together cover over 5,000 vulnerabilities across various applications. Reinforcement learning algorithms were implemented to simulate real-world penetration testing scenarios, allowing the AI agent to learn optimal strategies for exploiting vulnerabilities [49].

The framework also integrated tools such as Metasploit, Burp Suite, and TensorFlow to provide comprehensive testing capabilities [50]. The outcomes of this project were remarkable. The framework reduced the average time for penetration testing by 40% compared to traditional manual approaches. It also identified 15% more vulnerabilities, particularly in critical areas such as SQL injection, cross-site scripting (XSS), and server misconfigurations. Furthermore, the framework automated the generation of comprehensive vulnerability assessment reports, delivering results within 30 seconds—significantly faster than the industry average of 5 -

[16]https://www.unsw.edu.au/.

10 minutes. These reports were tailored to be accessible to both technical and non-technical stakeholders, ensuring clarity and usability [51]. Supporting data further validated the framework's success. A testbed of 50 web applications was created to evaluate its performance, where it successfully uncovered vulnerabilities that traditional tools like Burp Suite and Metasploit had missed. Reinforcement learning models achieved a 95% reward score in simulation environments, demonstrating their ability to optimize attack strategies. The framework was also tested in collaboration with a leading Australian cybersecurity firm, where it identified critical vulnerabilities in 3 out of 10 audited applications that had previously passed manual reviews [52]. The success of UNSW's AI-powered penetration testing framework highlights the effectiveness of the university's practical focus on cybersecurity education. By combining advanced AI methodologies, comprehensive datasets, and real-world validation, UNSW provides students with the skills to address emerging cybersecurity threats. This project underscores the transformative potential of integrating AI into cybersecurity education, preparing future professionals to excel in an increasingly dynamic and challenging field [53].

7. Proposed Framework for Integration and Methodology for Designing AI-Integrated Cybersecurity Courses

To address the challenges outlined, this paper proposes a multi-dimensional framework to effortlessly integrate AI into cybersecurity education. This framework aims to equip students with the skills needed to tackle emerging threats through three key pillars: curriculum design, hands-on training, and faculty development.

8. Curriculum Design

A well-structured curriculum forms the foundation for successful integration. This framework adopts a tiered approach:

8.1. Foundational Courses

Foundational courses introduce students to the fundamentals of AI, laying the groundwork for understanding and applying advanced concepts. These courses cover essential topics such as machine learning, data science, and their intersections with core cybersecurity concepts. Students are exposed to practical scenarios and real-world examples to solidify their understanding of abstract concepts [54]. For example, the analysis of datasets from network logs to identify potential threats or simulate encryption and decryption processes to understand cryptographic vulnerabilities [55]. Additionally, foundational courses emphasize collaboration and interdisciplinary approaches. Students work on team-based projects where they can integrate AI principles with cybersecurity frameworks to solve simplified versions of real-world problems. By establishing this strong foundation, students are prepared to tackle more specialized and advanced topics with confidence, ensuring a comprehensive understanding of both AI and cybersecurity

concepts [56].

As shown in Table 6, key topics in AI-driven cybersecurity include machine learning, which encompasses supervised, unsupervised, and reinforcement learning principles. Data science focuses on processing, visualization, and statistical analysis of large datasets. Network security explores AI applications in detecting and mitigating vulnerabilities, while cryptography examines how AI can optimize cryptographic algorithms and identify potential weaknesses.

Table 6. Topics and descriptions for foundational courses.

Topic	Description
Machine Learning	Principles of supervised, unsupervised, and reinforcement learning.
Data Science	Data processing, visualization, and statistical analysis for large datasets.
Network Security	Applications of AI in detecting and mitigating network vulnerabilities.
Cryptography	Use of AI to optimize cryptographic algorithms and identify weaknesses.

8.2. Advanced Modules

Advanced modules investigate into specialized AI applications in cybersecurity, equipping students with expertise directly applicable to tackling complex challenges. These modules are crucial because they bridge the gap between theoretical knowledge and practical implementation. By focusing on real-world applications, they ensure that students are prepared to address the dynamic and evolving nature of cybersecurity threats [57]. For instance, the Threat Intelligence Systems module empowers students to harness machine learning to process large-scale threat data, enabling the prediction and prevention of cyberattacks [58]. Behavioral Analysis focuses on anomaly detection to identify malicious activities that deviate from normal patterns, providing essential skills to counter sophisticated threats [59]. Automated Response Systems emphasize the automation of incident response, allowing organizations to react swiftly and effectively to mitigate damages [60].

These modules are complemented by industry collaboration, ensuring students gain insights into the practical deployment of these tools. As shown in Table 7, key modules in AI-driven cybersecurity include threat intelligence systems, which leverage machine learning to process threat data, identify patterns, and predict cyberattacks. Behavioral analysis focuses on using AI to detect anomalies in user behavior, network traffic, and system activities. Automated response systems are designed to develop AI-driven solutions for incident management, including threat isolation and system recovery.

Table 7. Modules and focus areas for advanced courses.

Module	Focus Areas
Threat Intelligence Systems	Processing threat data with machine learning to identify patterns and predict cyberattacks.
Behavioral Analysis	Using AI to detect anomalies in user behavior, network traffic, and system activities.
Automated Response Systems	Developing AI solutions for incident management, including threat isolation and system recovery.

8.3. Capstone Projects

Capstone projects serve as a culmination of the curriculum, encouraging students to tackle real-world cybersecurity challenges by applying their AI knowledge and skills [61]. These projects are essential as they provide a platform for students to demonstrate their problem-solving capabilities, creativity, and technical expertise. By simulating real-world scenarios, capstone projects ensure that students are job-ready and capable of addressing complex cybersecurity challenges upon graduation [62]. For example, projects like Phishing Detection Models teach students to design advanced NLP solutions to combat one of the most common cyber threats. Predictive Analytics tools help students anticipate and proactively counter cyber risks, while Incident Response Simulations allow them to practice managing and neutralizing active threats. Security Automation Frameworks prepare students to streamline routine cybersecurity operations, ensuring efficiency and scalability in professional environments [63]. Capstone projects also integrate industry feedback and mentorship, allowing students to refine their solutions and align them with current cybersecurity standards. Public presentations further enhance their communication and stakeholder engagement skills, making them well-rounded professionals.

Table 8. Capstone project examples and descriptions.

Project	Description
Phishing Detection Models	Design NLP models to analyze email content and detect phishing attempts.
Predictive Analytics	Create tools that forecast cyber threats by analyzing historical data and trends.
Incident Response Simulations	Develop AI-driven systems to simulate and manage cyberattacks for resilience testing.
Security Automation Frameworks	Build platforms to automate tasks like vulnerability scanning and patch management using AI algorithms.

As shown in Table 8, key AI-driven cybersecurity projects include phishing detection models, which utilize natural language processing (NLP) to analyze email content and identify phishing attempts. Predictive analytics focuses on developing tools that forecast cyber threats by analyzing historical data and trends. Incident response simulations involve AI-driven systems designed to simulate and manage cyberattacks for resilience testing. Security automation frameworks aim to automate tasks such as vulnerability scanning and patch management using AI algorithms.

9. Impact Assessment

Evaluating the effectiveness of AI integration within the program is essential to ensure its success. This framework employs a comprehensive three-pronged approach, focusing on Student Outcomes, Industry Feedback, and Continuous Improvement to maintain relevance, quality, and impact [64].

9.1. Student Outcomes

Measuring student outcomes provides tangible evidence of the program's impact on graduates' preparedness for the workforce. A significant proportion secure roles in cybersecurity or AI-focused positions shortly after graduation, highlighting the program's effectiveness in meeting industry demands. Alumni also show impressive job stability, with many remaining in their roles for over a year, reflecting the alignment of academic training with workforce requirements. Compared to the national average placement rate for similar programs, this program consistently outperforms, showcasing its impact on graduate success. A decade ago, technologies like generative artificial intelligence (GenAI) [65] and blockchain [66] were either speculative concepts or nonexistent. Today, they are mainstream, bringing both innovation and new security vulnerabilities. As these technologies reshape industries, they also transform the demand for cybersecurity expertise. According to research from IBM Corp. and the Ponemon Institute, the average cost of a security breach hit $4.88 million in 2024, a 10% increase from the previous year—the highest on record [67]. This escalating financial risk reinforces why corporations are aggressively recruiting cybersecurity professionals. Industry projections from IDC indicate that spending on security products will sustain double-digit growth over the next five years, reflecting the growing emphasis on cyber defense. Meanwhile, CompTIA's Cyberseek[17] tool reports that between May 2023 and April 2024, nearly 500,000 cybersecurity job openings emerged in the U.S. alone [68]. The sector is expanding at 267% the pace of overall job growth, underscoring the urgent need for skilled cybersecurity talent [69]. Figure 2 illustrates key cybersecurity trends, including the rising cost of security breaches [70]-[72].

[17]https://www.cyberseek.org/.

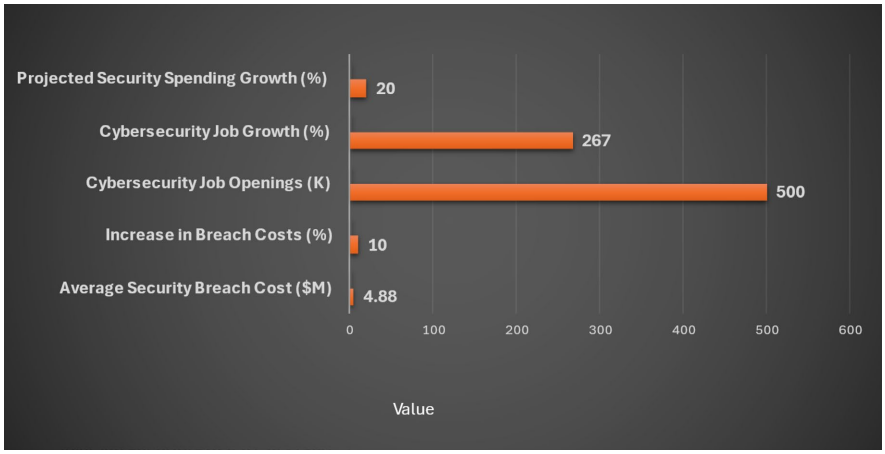

Figure 2. Key cybersecurity trends and statistics (2024).

9.2. Industry Feedback

The 2024 ISC2 Cybersecurity Workforce Study highlights how economic pressures and artificial intelligence (AI) are reshaping the cybersecurity profession, presenting both opportunities and challenges [73]. To stay ahead of evolving threats, organizations must acknowledge the obstacles their cybersecurity teams face, including staffing shortages and widening skills gaps. At the same time, it is crucial to recognize the progress made in strengthening the cybersecurity workforce. Expanding the global skills base enhances overall security, and ongoing investment in professional development—through training, conferences, certifications, and dedicated learning time—should be seen as a strategic necessity rather than a discretionary expense. These efforts are essential for building resilient teams capable of adapting to an increasingly complex threat landscape. As AI becomes a central driver of innovation, organizations must also account for the risks it introduces. Secure AI adoption requires more than just technical expertise—it demands careful planning, strong governance, ethical safeguards, privacy controls, and a deep understanding of evolving regulations. Cybersecurity professionals play a key role in managing these risks, reinforcing their importance as strategic leaders in protecting digital infrastructure. Despite the rising demand for cybersecurity professionals, workforce growth has slowed for the first time since ISC2 began tracking industry trends six years ago. Two consecutive years of reduced investment in hiring and professional development have led to significant talent shortages, with many organizations reporting heightened security risks. As businesses continue to integrate AI and navigate emerging threats, prioritizing skills development and cultivating the next generation of cybersecurity experts is no longer optional—it is critical for long-term resilience and success. In 2024, cybersecurity professionals faced a complex landscape of challenges that reshaped their roles and responsibilities across industries. Economic instability, geopolitical tensions, supply chain vulnerabilities, failed software updates, and the rapid automation and digitalization of security tasks have highlighted cybersecurity's essential role in protecting organizations. These disruptions have also provided profes-

sionals with opportunities to showcase their expertise in mitigating risks and strengthening defenses. Yet, despite the increasing demand and clear recognition of cybersecurity's value, the global active workforce has stagnated at 5.5 million, signaling an urgent need for renewed investment in talent development and retention. However, the workforce gap has expanded significantly to 4.8 million, marking a 19% year-over-year increase. To meet global demand, an estimated 10.2 million professionals are needed, representing an 8.1% rise. Figure 3 presents key cybersecurity workforce metrics, showing that the active cybersecurity workforce [74].

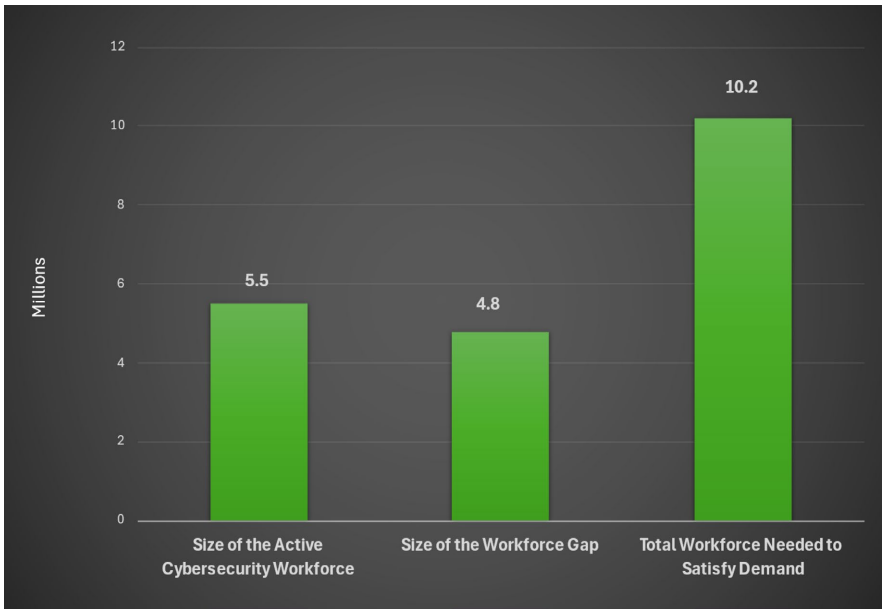

Figure 3. Global cybersecurity workforce trends (2024).

9.3. Internship Outcomes

Internship programs play a pivotal role in shaping the future cybersecurity workforce, equipping students with the hands-on experience needed to bridge the industry's skills gap [75]. As organizations across various sectors increasingly rely on cybersecurity to protect the integrity, confidentiality, and availability of information, the demand for qualified professionals continues to grow. Yet, with 700,000 unfilled cybersecurity positions in the United States, traditional pathways alone are insufficient in preparing graduates for the workforce [76]. The emergence of artificial intelligence (AI) is rapidly transforming cybersecurity, enabling advanced threat detection, predictive analytics, and automated responses. By integrating AI-driven security practices into internship experiences, students gain exposure to cutting-edge technologies that enhance their employability. Internship outcomes demonstrate that students who engage in AI-augmented cybersecurity roles are more likely to transition into full-time employment, as they develop critical skills aligned with industry needs [77]. A well-structured internship program that incorporates AI tools and real-world cybersecurity challenges not

only strengthens students' technical capabilities but also directly addresses workforce shortages. Employers increasingly prioritize candidates with hands-on experience in AI-driven security solutions, making internship participation a key differentiator in securing job offers. Expanding internship opportunities in cybersecurity—particularly those focused on AI applications—ensures that graduates are workforce-ready, effectively closing the gap between education and employment [78].

10. Conclusions

The integration of Artificial Intelligence (AI) into cybersecurity education is imperative for developing a workforce capable of combating the increasing complexity of digital threats. As cyberattacks become more sophisticated, traditional approaches to cybersecurity education are no longer sufficient. AI offers transformative capabilities, from real-time threat detection to automated response mechanisms, equipping professionals with the tools needed to anticipate and mitigate evolving risks. However, the successful adoption of AI in cybersecurity education requires overcoming significant challenges, including resource limitations, faculty expertise gaps, and the need for a modernized curriculum that aligns with industry standards.

Addressing these barriers requires a strategic approach. Higher education institutions must invest in AI-driven curricula that balance theoretical knowledge with hands-on experience, ensuring students gain proficiency in machine learning, behavioral analysis, and AI-assisted security automation. Faculty development programs and industry collaborations will be essential in bridging the expertise gap, enabling educators to incorporate emerging AI technologies effectively. Furthermore, fostering partnerships between academia and the private sector can provide students with access to real-world data, cutting-edge tools, and internship opportunities that enhance their job readiness. Beyond technical proficiency, cybersecurity education must instill adaptability, ethical responsibility, and a forward-thinking mindset. As AI continues to reshape the cybersecurity landscape, professionals must be prepared not only to operate advanced security systems but also to critically assess their implications, ensuring that AI-driven security solutions are deployed responsibly and equitably. Ultimately, integrating AI into cybersecurity education represents more than just an academic evolution—it is a fundamental shift in how the next generation of cybersecurity professionals will be trained. Institutions that embrace this transformation will play a pivotal role in securing the digital future, equipping graduates with the skills, knowledge, and resilience needed to defend against increasingly sophisticated cyber threats. The future of cybersecurity depends on a well-prepared workforce, and AI-driven education is the key to making that future a reality.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] George, A.S. and George, A.H. (2024) Riding the Wave: An Exploration of Emerging Technologies Reshaping Modern Industry. *Partners Universal International Innovation Journal*, **2**, 15-38.

[2] Kalinaki, K. (2024) Ransomware Threat Mitigation Strategies for Protecting Critical Infrastructure Assets. In: Kalinaki, K., Ed., *Ransomware Evolution*, CRC Press, 120-143. https://doi.org/10.1201/9781003469506-10

[3] Ghaffar, A., Arshad, A., Abbas, S. and Tahir, M. (2024) Artificial Intelligence in Information Technology: Enhancing Efficiency, Security, and Innovation: A Descriptive Review. *Spectrum of Engineering Sciences*, **2**, 289-309.

[4] Sarker, I.H. (2024) Introduction to Ai-Driven Cybersecurity and Threat Intelligence. In: Sarker, I.H., Ed., *AI-Driven Cybersecurity and Threat Intelligence*, Springer Nature Switzerland, 3-19. https://doi.org/10.1007/978-3-031-54497-2_1

[5] Belhadi, A., Mani, V., Kamble, S.S., Khan, S.A.R. and Verma, S. (2021) Artificial Intelligence-Driven Innovation for Enhancing Supply Chain Resilience and Performance under the Effect of Supply Chain Dynamism: An Empirical Investigation. *Annals of Operations Research*, **333**, 627-652. https://doi.org/10.1007/s10479-021-03956-x

[6] Sağlam, R.B., Miller, V. and Franqueira, V.N.L. (2023) A Systematic Literature Review on Cyber Security Education for Children. *IEEE Transactions on Education*, **66**, 274-286. https://doi.org/10.1109/te.2022.3231019

[7] Schmitt, M. and Flechais, I. (2024) Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing. *Artificial Intelligence Review*, **57**, Article No. 324. https://doi.org/10.1007/s10462-024-10973-2

[8] Khan, A., Jhanjhi, N., Hamid, D.H.H., Omar, H.A.H.B.H., Amsaad, F. and Wassan, S. (2025) Future Trends and Challenges in Cybersecurity and Generative AI. *Reshaping CyberSecurity with Generative AI Techniques*, 491-522. https://doi.org/10.4018/979-8-3693-5415-5.ch014

[9] Ali, J., Singh, S.K., Jiang, W., Alenezi, A.M., Islam, M., Daradkeh, Y.I. and Mehmood, A. (2025) A Deep Dive into Cybersecurity Solutions for AI-Driven IoT-Enabled Smart Cities in Advanced Communication Networks. *Computer Communications*, **229**, Article ID: 108000. https://doi.org/10.1016/j.comcom.2024.108000

[10] Alam, A. and Mohanty, A. (2023) Educational Technology: Exploring the Convergence of Technology and Pedagogy through Mobility, Interactivity, AI, and Learning Tools. *Cogent Engineering*, **10**, Article ID: 2283282. https://doi.org/10.1080/23311916.2023.2283282

[11] Uspenskyi, S. (2025) How Many AI Companies Will There Be in 2025 (Latest AI statistics). Springs. https://springsapps.com/knowledge/how-many-ai-companies-will-there-be-in-2024-latest-ai-statistics

[12] Gartner (2025) Gartner Forecasts Worldwide IT Spending to Grow 9.8% in 2025. Gartner Newsroom. https://www.gartner.com/en/newsroom/press-releases/2025-01-21-gartner-forecasts-worldwide-it-spending-to-grow-9-point-8-percent-in-2025

[13] Berger, G., Dawson, N. AND Yuan, A. (2024) AI's Expanding Reach: Mapping the Spread of AI Skills across America. https://static1.squarespace.com/static/6197797102be715f55c0e0a1/t/672cceeb32cb4a7a5c8d0b38/1730989803141/AI+Bulletin+OCT2024+-+Final2.pdf

[14] Weiner, S., Lake, R. AND Rosner, J. (2024) AI Is Evolving, but Teacher Prep Is Lagging: A First Look at Teacher Preparation Program Responses to AI. Center on Reinventing Public Education. https://crpe.org/

[15] Elkhatat, A.M., Elsaid, K. and Almeer, S. (2023) Evaluating the Efficacy of AI Content Detection Tools in Differentiating between Human and AI-Generated Text. *International Journal for Educational Integrity*, **19**, Article No. 17. https://doi.org/10.1007/s40979-023-00140-5

[16] Palmer, K. (2024) Most Campus Tech Leaders Say Higher Ed Is Unprepared for AI's Rise. Inside Higher Ed. https://www.insidehighered.com/news/tech-innovation/artificial-intelligence/2024/10/16/campus-tech-leaders-say-higher-ed

[17] Morgan, S. (2021) Cybersecurity Jobs Report: 3.5 Million Unfilled Positions in 2025. Cybersecurity Ventures. https://cybersecurityventures.com/jobs-report-2021/

[18] Lascaze, E., Corduneanu, R., Kreit, B., Cantrell, S., Kulkarni, A. and Rifkin, D. (2024) AI in the Workplace. Deloitte Insights. Deloitte Center for Integrated Research. https://www2.deloitte.com/us/en/insights/topics/talent/ai-in-the-workplace.html

[19] Law, M. (2024) O'Reilly: Bridging the Cybersecurity Skills Gap. Cyber Magazine. https://cybermagazine.com/articles/global-survey-reveals-critical-ai-security-skills-shortage

[20] Sniderman, B., Kearns-Manolatos, D. and Thomas, C. (2024) Gen AI Investment Opportunities Center on Data, Cybersecurity, and Cloud, Deloitte Survey Finds. Deloitte Insights. https://www2.deloitte.com/us/en/insights/topics/emerging-technologies/ai-investment-opportunities-tech-ecosystem.html

[21] Inside Higher Ed (2024) 2024 Survey of Campus Chief Technology/Information Officers. https://www.insidehighered.com/reports/2024/10/14/2024-survey-campus-chief-technologyinformation-officers

[22] Ponemon Institute (2024) State of AI in Cybersecurity 2024. https://mixmode.ai/state-of-ai-in-cybersecurity-2024-download/

[23] Lakshman Havish, K. (2024) Cybersecurity in Higher Education: A Roadmap for Universities to Prepare for the AI Era. CXOtoday. https://cxotoday.com/story/cybersecurity-in-higher-education-a-roadmap-for-universities-to-prepare-for-the-ai-era/

[24] Lu, M. (2024) AI Is Much More of an Opportunity than a Threat to Universities. Times Higher Education. https://www.timeshighereducation.com/blog/ai-much-more-opportunity-threat-universities

[25] Roessler, A. (2024) Universities Prepare Students for Life and Work in an AI World. MinnPost. https://www.minnpost.com/education/2024/11/universities-prepare-students-for-life-and-work-in-an-ai-world/

[26] Southworth, J., Migliaccio, K., Glover, J., Glover, J., Reed, D., McCarty, C., *et al.* (2023) Developing a Model for AI across the Curriculum: Transforming the Higher Education Landscape via Innovation in AI Literacy. *Computers and Education: Artificial Intelligence*, **4**, Article ID: 100127. https://doi.org/10.1016/j.caeai.2023.100127

[27] Carnegie Mellon University, Heinz College. (n.d.). 95-767: Principles of Computing. https://www.heinz.cmu.edu/current-students/courses/95-767/

[28] Camacho, N.G. (2024) The Role of AI in Cybersecurity: Addressing Threats in the

Digital Age. *Journal of Artificial Intelligence General Science*, **3**, 143-154. https://doi.org/10.60087/jaigs.v3i1.75

[29] CICIDS2017 Dataset (2017) Canadian Institute for Cybersecurity Intrusion Detection System Dataset 2017. https://www.unb.ca/cic/datasets/ids-2017.html

[30] Zoghi, Z. and Serpen, G. (2023) unsw-nb15 Computer Security Dataset: Analysis through Visualization. *Security and Privacy*, **7**, e331. https://doi.org/10.1002/spy2.331

[31] Dube, R. (2023) Faulty Use of the CIC-IDS 2017 Dataset in Information Security Research. *Journal of Computer Virology and Hacking Techniques*, **20**, 203-211. https://doi.org/10.1007/s11416-023-00509-7

[32] Ansel, J., Yang, E., He, H., Gimelshein, N., Jain, A., Voznesensky, M., *et al.* (2024) PyTorch 2: Faster Machine Learning through Dynamic Python Bytecode Transformation and Graph Compilation. *Proceedings of the* 29*th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*, La Jolla, 27 April 27-1 May 2024., 929-947. https://doi.org/10.1145/3620665.3640366

[33] Detection, A., Mehta, T., Kachhoria, R., Jaiswal, S., Kale, S., Kannan, R. and Mahajan, R.A. (2024) 17 Emails Classification. Data-Centric Artificial Intelligence for Multidisciplinary Applications, 271.

[34] Liu, F. and Panagiotakos, D. (2022) Real-World Data: A Brief Review of the Methods, Applications, Challenges and Opportunities. *BMC Medical Research Methodology*, **22**, Article No. 287. https://doi.org/10.1186/s12874-022-01768-6

[35] Regulwar, G.B., Mahalle, A., Pawar, R., Shamkuwar, S.K., Kakde, P.R. and Tiwari, S. (2024) Big Data Collection, Filtering, and Extraction of Features. In: Darwish, D., Ed., *Big Data Analytics Techniques for Market Intelligence*, IGI Global, 136-158. https://doi.org/10.4018/979-8-3693-0413-6.ch005

[36] Mujahid, M., Rustam, F., Shafique, R., Chunduri, V., Villar, M.G., *et al.* (2023) Analyzing Sentiments Regarding ChatGPT Using Novel BERT: A Machine Learning Approach. *Information*, **14**, Article 474. https://doi.org/10.3390/info14090474

[37] Jáñez-Martino, F., Alaiz-Rodríguez, R., González-Castro, V., Fidalgo, E. and Alegre, E. (2022) A Review of Spam Email Detection: Analysis of Spammer Strategies and the Dataset Shift Problem. *Artificial Intelligence Review*, **56**, 1145-1173. https://doi.org/10.1007/s10462-022-10195-4

[38] Altwaijry, N., Al-Turaiki, I., Alotaibi, R. and Alakeel, F. (2024) Advancing Phishing Email Detection: A Comparative Study of Deep Learning Models. *Sensors*, **24**, Article 2077. https://doi.org/10.3390/s24072077

[39] Arazzi, M., Arikkat, D.R., Nicolazzo, S., Nocera, A. and Conti, M. (2023) NLP-Based Techniques for Cyber Threat Intelligence. arXiv: 2311.08807.

[40] Kamalov, F., Santandreu Calonge, D. and Gurrib, I. (2023) New Era of Artificial Intelligence in Education: Towards a Sustainable Multifaceted Revolution. *Sustainability*, **15**, Article 12451. https://doi.org/10.3390/su151612451

[41] Xia, J., Li, M. and Li, J. (2024) Comparative Analysis Vision of Worldwide AI Courses. arXiv: 2407.16881. https://doi.org/10.48550/arXiv.2407.16881

[42] University of New South Wales. AI Guidelines and Framework. UNSW Teaching Gateway. https://www.teaching.unsw.edu.au/ai/guidelines

[43] ADAPT (2024) AI Transforms Australian Education with Enhanced Security and Privacy. https://adapt.com.au/resources/articles/digital-transformation/ai-transforms-australian-education-with-enhanced-security-and-privacy/

[44] Rouleau, N. and Murugan, N.J. (2024) The Risks and Rewards of Embodying Artifi-

cial Intelligence with Cloud-based Laboratories. *Advanced Intelligent Systems*, **7**, Article ID: 2400193. https://doi.org/10.1002/aisy.202400193

[45] Awiszus, K., Bell, Y., Lüttringhaus, J., Svindland, G., Voß, A. and Weber, S. (2023) Building Resilience in Cybersecurity: An Artificial Lab Approach. *Journal of Risk and Insurance*, **91**, 753-800. https://doi.org/10.1111/jori.12450

[46] Wang, T., Zhou, N. and Chen, Z. (2025) CyberMentor: AI Powered Learning Tool Platform to Address Diverse Student Needs in Cybersecurity Education. arXiv: 2501.09709.

[47] UNSW Sydney (2024) Educational Technology Roadmap 2024-2028. https://www.education.unsw.edu.au/news-events/news/educational-technology-roadmap-2024-2028

[48] Alaryani,, M., Alremeithi, S., Al Ali, F. and Ikuesan, R. (2024) Penthack: Ai-Enabled Penetration Testing Platform for Knowledge Development. *European Conference on Cyber Warfare and Security*, **23**, 27-36. https://doi.org/10.34190/eccws.23.1.2493

[49] Kaur, R., Gabrijelčič, D. and Klobučar, T. (2023) Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions. *Information Fusion*, **97**, Article ID: 101945.

[50] Alazmi, S. (2023) Enhancing the Performance of Web Application Security Testing: An In-Depth Analysis and Optimization of Web Vulnerability Scanners. Master's Thesis, University of Idaho.

[51] Altulaihan, E.A., Alismail, A. and Frikha, M. (2023) A Survey on Web Application Penetration Testing. *Electronics*, **12**, Article 1229. https://doi.org/10.3390/electronics12051229

[52] Jampani, S.K. (2024) Revolutionizing Penetration Testing: Ai-Powered Automation for Enterprise Security. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, **10**, 1562-1569. https://doi.org/10.32628/cseit241061201

[53] Chaudhary, P.S., Khurana, M.R. and Ayalasomayajula, M. (2024) Real-World Applications of Data Analytics, Big Data, and Machine Learning. In: Singh, P., Mishra, A.R. and Garg, P., Eds., *Data Analytics and Machine Learning*, Springer, 237-263. https://doi.org/10.1007/978-981-97-0448-4_12

[54] Nguyen, A., Kremantzis, M., Essien, A., Petrounias, I. and Hosseini, S. (2024) Editorial: Enhancing Student Engagement through Artificial Intelligence (AI): Understanding the Basics, Opportunities, and Challenges. *Journal of University Teaching and Learning Practice*, **21**. https://doi.org/10.53761/caraaq92

[55] Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A. and Akin, E. (2023) A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, **12**, Article 1333. https://doi.org/10.3390/electronics12061333

[56] Pokala, P. (2025) The Integration and Impact of Artificial Intelligence in Modern Enterprise Resource Planning Systems: A Comprehensive Review. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5069295

[57] Stamp, M. (2022) Introduction to Machine Learning with Applications in Information Security. 2nd Edition, Chapman and Hall/CRC. https://doi.org/10.1201/9781003264873

[58] Rana, S. and Chicone, R. (2025) Fortifying the future: Harnessing AI for Transformative Cybersecurity Training. Springer. https://doi.org/10.1007/978-3-031-81780-9

[59] Olabanji, S.O., Marquis, Y.A., Adigwe, C.S., Ajayi, S.A., Oladoyinbo, T.O. and Olaniyi, O.O. (2024) AI-Driven Cloud Security: Examining the Impact of User Be-

havior Analysis on Threat Detection. *Asian Journal of Research in Computer Science*, **17**, 57-74. https://doi.org/10.9734/ajrcos/2024/v17i3424

[60] Hassan, S.K. and Ibrahim, A. (2023) The Role of Artificial Intelligence in Cyber Security and Incident Response. *International Journal for Electronic Crime Investigation*, **7**, 49-72. https://doi.org/10.54692/ijeci.2023.0702154

[61] Nelson, C.D. (2024) Hacking the Learning Curve: Effective Cybersecurity Education at Scale. Arizona State University.

[62] Familoni, B.T. (2024) Cybersecurity Challenges in the Age of AI: Theoretical Approaches and Practical Solutions. *Computer Science & IT Research Journal*, **5**, 703-724. https://doi.org/10.51594/csitrj.v5i3.930

[63] He, K., Kim, D.D. and Asghar, M.R. (2023) Adversarial Machine Learning for Network Intrusion Detection Systems: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, **25**, 538-566. https://doi.org/10.1109/comst.2022.3233793

[64] González-Pérez, L.I. and Ramírez-Montoya, M.S. (2022) Components of Education 4.0 in 21st Century Skills Frameworks: Systematic Review. *Sustainability*, **14**, Article 1493. https://doi.org/10.3390/su14031493

[65] Law, L. (2024) Application of Generative Artificial Intelligence (GenAI) in Language Teaching and Learning: A Scoping Literature Review. *Computers and Education Open*, **6**, Article ID: 100174. https://doi.org/10.1016/j.caeo.2024.100174

[66] Zheng, Z., Xie, S., Dai, H.N., Chen, X. and Wang, H. (2018) Blockchain Challenges and Opportunities: A Survey. *International Journal of Web and Grid Services*, **14**, 352-375. https://doi.org/10.1504/ijwgs.2018.095647

[67] IBM (2024) IBM Report: Escalating Data Breach Disruption Pushes Costs to New Highs. IBM Newsroom. https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs

[68] CompTIA (2024) State of Cybersecurity 2025: Developing Strategy Using Enterprise Architecture. CompTIA. https://www.comptia.org/content/research/cybersecurity-trends-research

[69] AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F. and Raymond Choo, K. (2022) The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education. *Computers & Security*, **119**, Article ID: 102754. https://doi.org/10.1016/j.cose.2022.102754

[70] Webb, D. (2024) Top 9 Trends in Cybersecurity Careers for 2025. eSecurity Planet. https://www.esecurityplanet.com/trends/cybersecurity-careers/

[71] Creese, S. and Joshi, A. (2025) Securing Innovation: A Leader's Guide to Managing Cyber Risks from AI Adoption. World Economic Forum. https://www.weforum.org/stories/2025/01/a-leaders-guide-to-managing-cyber-risks-from-ai-adoption/

[72] Institute of Data (2024) Careers in Cybersecurity: Transitioning in 2025. Institute of Data. https://www.institutedata.com/us/blog/careers-in-cybersecurity-transitioning-in-2025/

[73] International Information System Security Certification Consortium (ISC2) (2024) Global Cybersecurity Workforce Prepares for an AI-Driven World: 2024 ISC2 Cybersecurity Workforce Study. ISC2. https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

[74] International Information System Security Certification Consortium (2024) Employ-

ers Must Act as Cybersecurity Workforce Growth Stalls and Skills Gaps Widen. ISC2. https://www.isc2.org/Insights/2024/09/Employers-Must-Act-Cybersecurity-Workforce-Growth-Stalls-as-Skills-Gaps-Widen

[75] Creese, S. and Jurgens, J. (2025) Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards. World Economic Forum. https://reports.weforum.org/docs/WEF_Artificial_Intelligence_and_Cybersecurity_Balancing_Risks_and_Rewards_2025.pdf

[76] Wu, M. (2024) Introducing the Cyber Jobs Dataset. Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/introducing-the-cyber-jobs-dataset/

[77] Wong, H., Chang, A. and Pugh, B. (2024) The Transformative Role of AI in Cybersecurity: Anticipating and Preparing for Future Applications and Benefits. R Street Institute. https://www.rstreet.org/commentary/the-transformative-role-of-ai-in-cybersecurity-anticipating-and-preparing-for-future-applications-and-benefits/

[78] Jurgens, J. and Dal Cin, P. (2025) Global Cybersecurity Outlook 2025. World Economic Forum. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/