# Empowering the Next Generation: A Strategic Roadmap for AI in Cybersecurity Education

Vahid Heydari
*Computer Science Department*
*Morgan State University*
Baltimore, USA
vahid.heydari@morgan.edu
0000-0002-6181-6826

Kofi Nyarko
*Electrical and Computer Engineering Department*
*Morgan State University*
Baltimore, USA
kofi.nyarko@morgan.edu
0000-0002-7481-5080

***Abstract***—The integration of artificial intelligence (AI) into cybersecurity is revolutionizing how institutions address increasingly complex cyber threats. As the demand for expertise in both AI and cybersecurity grows, Historically Black Colleges and Universities (HBCUs) have a unique opportunity to develop programs that equip students with the necessary skills to meet these evolving challenges. This paper presents a strategic roadmap for developing AI in Cybersecurity programs at HBCUs, emphasizing interdisciplinary collaboration, hands-on learning, adversarial defense, explainability, ethical leadership, and diversity. To strengthen the roadmap, this paper incorporates real-world case studies from existing AI-cybersecurity programs and proposes strategies to overcome key challenges such as faculty expertise gaps, funding limitations, and resource scalability. Additionally, a framework for evaluating program effectiveness is introduced, offering measurable metrics such as student outcomes, industry collaboration, and curriculum adaptability. By implementing this roadmap, HBCUs can establish sustainable AI in Cybersecurity programs that align with industry needs while fostering leadership and innovation in the cybersecurity workforce.

***Keywords***—*Artificial Intelligence (AI), Cybersecurity, Machine Learning (ML), Adversarial Attacks, Model Explainability, Generative Adversarial Networks (GANs), Historically Black Colleges and Universities (HBCUs), Interdisciplinary Education*

## I. INTRODUCTION

The rapid advancement of artificial intelligence (AI) has significantly transformed cybersecurity, with increasingly complex digital infrastructures leading to more sophisticated cyber threats. This evolving landscape necessitates a new breed of cybersecurity professionals who are proficient not only in traditional security practices but also in leveraging AI and Machine Learning (ML) to enhance threat detection, response, and prevention.

This work is supported in part by the Center for Equitable Artificial Intelligence and Machine Learning Systems (CEAMLS) at Morgan State University. Generative AI and automated tools were used to assist in the production of this paper, but no AI tools were credited as authors, in accordance with the submission guidelines.

AI's integration into cybersecurity has greatly strengthened organizational defenses, enabling the rapid detection and response to threats like ransomware, thereby minimizing damage and improving efficiency [1]. AI also automates essential but time-consuming security tasks, such as log analysis and anomaly detection, allowing cybersecurity teams to shift their focus to strategic and high-priority initiatives [2]. Moreover, AI's scalability enables protection across expanding digital infrastructures without requiring a proportional increase in human resources [3].

Among AI's most significant contributions is its predictive capability, which allows organizations to anticipate and mitigate cyber threats before they materialize. By analyzing large volumes of security data, AI can detect patterns and anomalies indicative of potential attacks, giving organizations the ability to fortify defenses proactively [4]. This transition from reactive to proactive cybersecurity represents a paradigm shift in digital security management.

Despite these advancements, the integration of AI in cybersecurity presents challenges. AI models often operate as "black boxes," making it difficult to interpret their decision-making processes, which raises concerns about trust, accountability, and security. Explainability methods, such as SHAP [5] and LIME [6], help demystify AI decision-making and improve transparency in high-stakes applications like cybersecurity. Additionally, adversaries are increasingly leveraging AI to generate adversarial samples designed to bypass detection systems, leading to an ongoing arms race between attackers and defenders. Researchers have explored defenses using Generative Adversarial Networks (GANs) to create robust models capable of resisting adversarial attacks [7], [8]. Given these challenges, educational programs must evolve to equip students with both the technical expertise to harness AI-driven security tools and the analytical skills to navigate the ethical and societal implications of AI in cybersecurity.

Historically Black Colleges and Universities (HBCUs) are well-positioned to address these challenges by developing comprehensive AI in Cybersecurity programs that not only meet industry demands but also emphasize interdisciplinary education, diversity, and ethical responsibility. HBCUs have a

long-standing tradition of fostering inclusion and equity in STEM fields, making them ideal institutions for training a new generation of cybersecurity professionals who are technically proficient, socially conscious, and ethically grounded. However, HBCUs often face barriers such as funding limitations, faculty expertise gaps, and resource constraints, which must be considered when designing AI in Cybersecurity programs. This paper presents a strategic roadmap for AI in Cybersecurity education at HBCUs, emphasizing interdisciplinary collaboration, practical applications, adversarial defense techniques, and ethical considerations. The roadmap incorporates real-world case studies and outlines strategies for overcoming common challenges such as resource scalability and faculty upskilling. Furthermore, a framework for evaluating the success of AI in Cybersecurity programs is proposed, including measurable metrics such as student career outcomes, curriculum adaptability, and industry collaborations. By implementing this roadmap, HBCUs can establish sustainable, high-impact AI-driven cybersecurity programs that prepare students for leadership roles, contribute to workforce diversity, and advance innovation in STEM.

## II. LITERATURE REVIEW

The development of an AI in Cybersecurity program at HBCUs, alongside broader efforts to establish interdisciplinary education in fields like AI and cybersecurity, requires a thorough review of existing literature. This section integrates insights from various studies to inform the design of an effective curriculum tailored to the unique challenges and opportunities in these domains. Additionally, it addresses key challenges such as resource constraints, faculty expertise, and the need for structured evaluation metrics to assess program success.

### *A. Integrating Machine Learning and AI into Cybersecurity Education*

Integrating AI and ML into cybersecurity education has become essential due to the increasing sophistication of cyber threats. Traditional cybersecurity measures alone are insufficient against modern attacks that exploit vulnerabilities in AI-driven systems. Machine learning plays a critical role in enhancing cybersecurity strategies through advanced threat detection, anomaly detection, and predictive analytics [9]. These technologies enable real-time identification of threats such as malware, phishing, and advanced persistent threats (APTs), which conventional rule-based systems might fail to detect.

Training students to handle adversarial attacks is crucial for preparing them for real-world cybersecurity challenges [10]. AI-driven attacks, particularly adversarial attacks, manipulate input data to deceive ML models, allowing attackers to bypass security systems undetected. By incorporating adversarial defense techniques into cybersecurity education, students can learn to recognize, mitigate, and develop countermeasures against such attacks.

Furthermore, cybersecurity education should not only focus on technical proficiency but also on ethical considerations such as bias, fairness, and accountability [11]. The implementation of AI-driven security tools raises concerns about the transparency and fairness of automated decision-making, necessitating a curriculum that balances technical expertise with responsible AI usage. Addressing these ethical concerns is vital for fostering responsible cybersecurity professionals who can navigate the legal and societal implications of AI in security contexts.

Additionally, integrating AI and ML into cybersecurity education facilitates a transition from reactive security measures to proactive defense strategies. AI-powered analytics enable cybersecurity professionals to anticipate and mitigate cyber risks before they materialize, reducing the potential for breaches. As organizations increasingly rely on AI-enhanced security frameworks, graduates equipped with knowledge of AI in cybersecurity will be better prepared for the workforce.

### *B. Explainability and Adversarial Defense in Cybersecurity*

Explainability and adversarial defense are crucial components of AI-driven cybersecurity. The increasing complexity of ML models used in cybersecurity introduces challenges related to transparency and trust. Security analysts need explainable AI (XAI) techniques to understand how models classify threats and to detect adversarial manipulations effectively.

Explainable AI methods such as SHAP [5], LIME [6], and Partial Dependence Plots [12] have been adapted for cybersecurity applications to enhance model transparency. These methods allow analysts to determine which features contribute most to a model's classification decision, aiding in the identification of adversarial samples. Additionally, techniques like Integrated Gradients (IG) [13] and DeepLIFT [14] provide insights into deep learning models, improving trust and interpretability in AI-driven security solutions.

Adversarial attacks remain a significant challenge, as attackers develop techniques to evade AI-powered security measures by crafting adversarial samples [15]. These adversarial inputs manipulate ML models, leading to misclassification of malicious activity as benign. Defensive strategies such as adversarial training, defensive distillation, and GANs are essential to countering these attacks [7], [8]. GANs, for example, can be used to both generate and defend against adversarial malware samples, demonstrating their dual role in cybersecurity.

### *C. Hands-On and Project-Based Learning*

Practical, hands-on learning is crucial for preparing students to tackle real-world cybersecurity challenges. Traditional lecture-based instruction is insufficient for equipping students with the applied skills needed to implement AI-driven security solutions. Studies show that experiential learning through labs and real-world simulations

significantly improves student retention and problem-solving abilities [16], [17].

Hands-on approaches enable students to directly engage with AI-powered security tools, test adversarial models, and analyze explainability frameworks [18]. These experiences prepare students for the workforce by simulating real-world cybersecurity threats and enabling them to develop defensive strategies in controlled environments.

Despite the benefits of project-based learning, implementing such methodologies at HBCUs presents challenges, including limited access to AI cybersecurity tools and computing resources [19]. Addressing these barriers requires strategic integration of AI platforms into the curriculum, as well as collaborations with industry and research institutions.

### *D. Considerations for HBCU Context and Strategic Partnerships*

HBCUs play a crucial role in broadening participation in STEM fields, particularly in cybersecurity. However, they face systemic challenges related to funding, faculty expertise, and access to state-of-the-art technology. Studies highlight the importance of "strategic partnerships" between HBCUs and industry leaders to bridge these gaps and provide students with the necessary resources and training [20].

Effective cybersecurity education programs at HBCUs should leverage industry collaborations to provide access to real-world cybersecurity challenges and AI tools. Partnerships with private sector companies, government agencies, and research institutions enable HBCUs to offer "internships, guest lectures, sponsored projects, and training programs" that enhance student learning and professional development [21].

Faculty training is another critical factor in successfully integrating AI into cybersecurity curricula. Given the rapid evolution of AI and ML technologies, ongoing faculty development programs, such as AI boot camps, certifications, and cross-institutional training initiatives, can help educators stay up to date with emerging cybersecurity threats and mitigation techniques [22].

### *E. Broadening Participation and Interdisciplinary Education*

The integration of AI into cybersecurity is inherently interdisciplinary, requiring collaboration between computer science, data science, policy, and ethics. To address this, AI in Cybersecurity programs should incorporate "interdisciplinary coursework" that combines technical proficiency with policy and legal considerations [23]. Studies suggest that interdisciplinary approaches improve students' ability to understand cybersecurity threats from multiple perspectives, fostering well-rounded professionals [24].

Broadening participation in AI-cybersecurity programs is crucial for increasing diversity in the field. Initiatives such as "outreach programs, scholarship opportunities, and industry mentorships" can help attract underrepresented students to cybersecurity careers. Research demonstrates that HBCUs that actively implement diversity-focused cybersecurity initiatives see higher engagement and retention rates among minority students [25], [26].

### *F. Leadership in AI and Cybersecurity Education*

As AI continues to transform the cybersecurity landscape, cultivating leadership in AI education is essential. Developing leadership skills alongside technical expertise enables students to "drive AI innovation in cybersecurity fields" while navigating the ethical, legal, and societal implications of AI [27]. Integrating leadership training into AI-cybersecurity programs can help students take on managerial roles in cybersecurity strategy, policy development, and AI ethics.

### *G. Case Studies and Practical Insights for Curriculum Development*

Case studies provide valuable insights into the practical implementation of AI-cybersecurity curricula. Studies show that institutions that integrate real-world case studies into their curriculum produce graduates with stronger analytical and problem-solving skills [28]. Additionally, research highlights the effectiveness of "traveling concepts," which involves students applying interdisciplinary knowledge across different domains to tackle cybersecurity challenges [29].

## III. SUMMARY OF LITERATURE REVIEW FINDINGS

The reviewed literature underscores several key points relevant to the development of AI in Cybersecurity programs at HBCUs:

- AI and ML Integration: AI-driven cybersecurity tools are critical for modern threat detection, and students need hands-on exposure to these technologies.
- Explainability and Adversarial Defense: Teaching students how AI models make security-related decisions and how adversarial attacks work is essential for developing resilient defenses.
- Hands-on Learning: Project-based learning and cybersecurity simulations significantly enhance student engagement and preparedness.
- Strategic Partnerships: Collaborations between HBCUs and industry partners help bridge the resource and faculty expertise gap.
- Interdisciplinary Approach: Combining cybersecurity education with AI ethics, law, and policy enhances student readiness for industry roles.
- Diversity and Inclusion: Expanding AI-cybersecurity initiatives at HBCUs is vital for increasing diversity in cybersecurity and AI-related fields.

This literature review informs the roadmap proposed in this paper, ensuring that AI in Cybersecurity programs at HBCUs are aligned with industry needs while addressing educational challenges unique to these institutions.

## IV. METHODOLOGY

This study employs a systematic approach to reviewing existing literature and best practices in AI and cybersecurity education, with a particular emphasis on their relevance to HBCUs. The objective is to identify key themes, challenges, and opportunities that can inform the development of AI in Cybersecurity programs tailored to the unique context of HBCUs. The methodology follows a structured process to ensure a comprehensive and rigorous review of relevant materials, with a focus on interdisciplinary approaches, practical applications, and the inclusion of diverse perspectives to build robust and impactful educational programs.

### *A. Literature Selection Process*

To ensure a thorough and credible review, relevant academic papers, case studies, and reports were systematically selected from peer-reviewed journals, conference proceedings, and authoritative sources in cybersecurity and AI education. The selection process involved the following steps:

- **Keyword-Based Search:** Databases such as IEEE Xplore, ACM Digital Library, Google Scholar, and educational repositories were searched using keywords including "AI in cybersecurity education," "HBCU STEM programs," "interdisciplinary cybersecurity training," "adversarial defense education," and "AI ethics in cybersecurity."
- **Inclusion Criteria:** Papers were included if they (a) discussed AI or ML integration into cybersecurity curricula (b)examined interdisciplinary cybersecurity education, or (c) addressed challenges and strategies specific to HBCUs in STEM education.
- **Exclusion Criteria:** Older works that did not reflect recent advancements in AI-driven cybersecurity education were excluded, along with studies that did not focus on education-specific challenges.
- **Snowballing Method:** Additional references were identified by analyzing citations from the initially selected papers to ensure a comprehensive literature base.

### *B. Data Analysis and Synthesis*

The selected literature was analyzed to extract insights into successful strategies, common obstacles, and emerging trends that are applicable to the HBCU context. The analysis focused on the following core aspects:

- **Best Practices in AI-Cybersecurity Education:** Identifying pedagogical models that have successfully integrated AI and ML into cybersecurity training, emphasizing hands-on learning and practical applications.
- **Interdisciplinary Approaches:** Exploring studies that advocate for combining AI and cybersecurity with fields such as law, ethics, and business to create a more holistic educational framework.
- **Challenges and Opportunities for HBCUs:** Examining literature that discusses the institutional barriers faced by HBCUs, including funding constraints, faculty expertise gaps, and resource limitations.
- **Industry and Workforce Readiness:** Reviewing studies that highlight industry expectations for AI in cybersecurity roles and how education programs can be structured to align with workforce needs.

The insights derived from the literature were synthesized to create a flexible roadmap for the development of AI in Cybersecurity programs at HBCUs. This roadmap is designed as a set of guiding principles and strategic recommendations, rather than a prescriptive curriculum, allowing adaptation to the diverse needs of HBCUs. By emphasizing adaptability and responsiveness to the rapidly evolving landscape of AI and cybersecurity, the roadmap aims to serve as a dynamic tool for continuous improvement and innovation.

### *C. Validation Approach and Future Work*

To ensure the proposed roadmap is aligned with both academic standards and industry expectations, future work will involve gathering input from multiple stakeholders within the HBCU community and the broader cybersecurity industry. The validation approach includes:

- **Faculty and Curriculum Developers:** Conducting structured discussions with educators at HBCUs to assess feasibility, scalability, and alignment with institutional goals.
- **Industry Professionals:** Engaging with cybersecurity practitioners and AI experts to evaluate whether the roadmap meets workforce demands and reflects industry best practices.
- **Pilot Programs and Case Studies:** Identifying and studying existing AI in cybersecurity education initiatives to validate the roadmap's applicability.
- **Program Evaluation Metrics:** Developing clear assessment criteria, including student performance, employment outcomes, and curriculum adaptability, to measure the long-term success of AI in cybersecurity programs.

By integrating feedback from these stakeholders, the roadmap can evolve into a well-validated and actionable framework for establishing AI in Cybersecurity programs at HBCUs. This collaborative validation process will ensure that the recommendations remain relevant, scalable, and effective in addressing both educational and industry needs.

## V. DISCUSSION

The integration of AI into cybersecurity education presents a transformative opportunity for HBCUs to lead in preparing the next generation of cybersecurity professionals. The insights gathered from the literature review underscore the importance of developing AI in Cybersecurity programs that

leverage the unique strengths of HBCUs while addressing institutional challenges. This discussion highlights key themes and considerations that should guide the creation and implementation of these programs, emphasizing interdisciplinary collaboration, adversarial defense, model explainability, practical application, leadership development, and strategic partnerships. Additionally, challenges such as infrastructure limitations, faculty training, and funding concerns are discussed with potential strategies for mitigation.

### *A. Interdisciplinary Collaboration*

A key theme in AI-driven cybersecurity education is the necessity of interdisciplinary collaboration. AI and cybersecurity are inherently multidisciplinary fields, intersecting with computer science, engineering, ethics, law, and business. HBCUs, with their strong tradition of interdisciplinary education, are well-positioned to create programs that integrate these diverse fields.

By incorporating expertise from multiple disciplines, AI in Cybersecurity programs can provide students with a well-rounded perspective on security threats and solutions [25], [26]. Law and policy courses, for instance, can introduce students to the ethical and legal implications of AI-driven security measures, preparing them for roles that require both technical and regulatory expertise. Similarly, business and management courses can equip students with the leadership skills necessary for overseeing AI-security operations in large organizations.

One strategy for fostering interdisciplinary collaboration is the co-teaching model, where faculty members from different departments jointly develop and teach AI-security courses. Additionally, research projects that bring together faculty and students from multiple fields can create a dynamic learning environment that reflects real-world problem-solving.

### *B. Practical Application, Adversarial Defense, and Experiential Learning*

Practical application and experiential learning are crucial for bridging the gap between theoretical knowledge and real-world cybersecurity challenges. The literature supports the inclusion of hands-on labs, project-based courses, and real-world problem-solving activities as core components of these programs.

Students should engage in AI-driven cybersecurity challenges such as:

- Malware Detection: Training ML models to classify malicious software.
- Network Intrusion Prevention: Detecting and mitigating security breaches using AI-driven anomaly detection.
- Adversarial Sample Generation: Crafting adversarial examples using GANs to evaluate model robustness [7], [8].

Adversarial defense techniques are particularly important for training students to anticipate and mitigate AI-driven attacks. Implementing explainability techniques such as SHAP [5] and LIME [6] ensures that students can interpret and refine AI models, enhancing trust and accountability.

### *C. Addressing Resource Scalability and Faculty Training*

One of the biggest challenges for implementing AI in Cybersecurity programs at HBCUs is resource scalability, particularly in terms of computing infrastructure, faculty expertise, and funding. The paper has acknowledged these challenges, but further detail on overcoming them strengthens the roadmap:

- Leveraging Cloud-Based Computing: Many AI-security applications require high-performance computing resources. HBCUs can partner with cloud service providers (such as AWS, Microsoft Azure, or Google Cloud) to gain free or subsidized access to cloud-based tools for AI training.
- Faculty Development Programs: Upskilling faculty in AI-driven cybersecurity topics is essential. Collaborative initiatives like AI and cybersecurity boot camps for faculty, sabbatical programs in industry, or joint research projects can bridge this gap.
- Industry Partnerships for Equipment and Grants: Strategic collaborations with tech companies can provide funding for lab development, training workshops, and direct mentorship opportunities for students.

By addressing these institutional constraints, AI in Cybersecurity programs at HBCUs can remain scalable and sustainable, ensuring their long-term success.

### *D. Diversity and Inclusion in STEM Education*

Diversity and inclusion should be an explicit goal of AI in Cybersecurity programs at HBCUs. Studies emphasize the importance of representation in STEM fields, and AI-security education must reflect this commitment [20]. This can be achieved through:

- Scholarships and Fellowships for underrepresented students.
- Industry Mentorship Programs, where students connect with professionals from similar backgrounds.
- Bias and Fairness Training in AI, ensuring that students understand and mitigate bias in security models.

By emphasizing equity and inclusion, HBCUs can train cybersecurity professionals who bring diverse perspectives to security challenges, making AI systems more fair and effective.

### *E. Ethical Considerations, Leadership Development, and Explainability*

Cybersecurity professionals must not only be technically skilled but also ethically responsible. The rapid adoption of AI

introduces concerns such as algorithmic bias, surveillance ethics, and data privacy [27]. AI in Cybersecurity programs should incorporate coursework on AI ethics, training students to balance innovation with social responsibility.

Model explainability is particularly important in cybersecurity, where "black box" models must be interpretable to ensure trust. Explainability techniques such as SHAP, LIME, and Integrated Gradients [5], [6], [13] should be incorporated into coursework to help students develop AI systems that are both transparent and resilient.

### *F. Strategic Partnerships and Industry Collaboration*

Industry engagement plays a key role in ensuring that HBCU cybersecurity graduates are well-prepared for workforce demands. HBCUs should actively build partnerships with tech companies, government agencies, and research institutions to provide:

- Internships and Apprenticeships: Real-world experience working on AI-driven security challenges.
- Guest Lectures and Workshops: Professionals from the industry sharing best practices in cybersecurity.
- Co-Developed Curricula: Ensuring that academic programs align with industry needs.

Additionally, resource sharing among HBCUs can enhance capacity-building efforts. Consortium models—where multiple institutions pool resources and offer joint courses—can allow smaller HBCUs to access AI-focused cybersecurity programs.

### *G. Pilot Programs and Evaluation Metrics*

Pilot programs are essential for testing curriculum effectiveness before full-scale implementation. A semester-long pilot course in adversarial machine learning could involve:

- Practical Labs: Where students train, attack, and defend AI models.
- Industry Collaboration: Featuring guest lectures from AI-security professionals.
- Capstone Projects: Focused on real-world adversarial threats.

To ensure success, AI in Cybersecurity programs must have clear evaluation metrics, such as:

- Student Proficiency Assessments: Measuring competency in AI-security concepts.
- Employment Outcomes: Tracking job placement rates post-graduation.
- Industry Feedback Loops: Ensuring that HBCU graduates meet cybersecurity workforce needs.

### *H. Roadmap for Future Development*

The key insights from this discussion emphasize a strategic and comprehensive approach to developing AI in Cybersecurity programs at HBCUs. The roadmap does not propose a rigid curriculum but rather guiding principles that ensure flexibility, interdisciplinary collaboration, ethical responsibility, and real-world application.

By adopting this roadmap, HBCUs can establish themselves as leaders in AI-driven cybersecurity education while also addressing industry needs and preparing students to thrive in a rapidly evolving digital security landscape.

## VI. CONCLUSION

The integration of AI into cybersecurity presents a transformative opportunity for HBCUs to play a pivotal role in shaping the future of this critical field. As cyber threats grow in complexity, professionals who can blend traditional cybersecurity practices with AI-driven techniques are increasingly in demand. The ability to harness AI for threat detection, response, and prevention will be a defining factor in the effectiveness of future cybersecurity strategies.

This paper has outlined a strategic roadmap for developing AI in Cybersecurity programs at HBCUs, focusing on interdisciplinary collaboration, practical application, adversarial defense, ethical leadership, and inclusivity. These guiding principles are essential for designing flexible and adaptable educational programs that remain aligned with industry advancements, workforce demands, and the evolving nature of cyber threats.

Key insights from this roadmap emphasize the importance of:

- Experiential Learning & Hands-on Training – Incorporating practical labs, adversarial model testing, and AI-driven cybersecurity challenges ensures students gain real-world experience before entering the workforce.
- Explainability & Adversarial Defense – Training students to develop AI models that are resilient to adversarial attacks while ensuring transparency and accountability in cybersecurity applications.
- Ethical Considerations & Responsible AI Use – Embedding ethics into AI education to prepare students to address bias, fairness, and accountability in AI-driven security models.
- Industry & Research Partnerships – Strengthening collaborations with tech firms, government agencies, and academic institutions to provide students with internships, research opportunities, and real-world case studies.
- Scalability & Sustainability – Leveraging cloud-based resources, faculty development programs, and interdisciplinary course-sharing models to overcome infrastructure and funding challenges.
- Evaluation & Continuous Improvement – Establishing assessment criteria for program effectiveness, including student performance metrics, employment outcomes, and feedback loops from industry partners.

By emphasizing these elements, HBCUs can establish themselves as leaders in AI-driven cybersecurity education, fostering a diverse and inclusive workforce equipped to address emerging cyber threats. The roadmap provides HBCUs with a structured yet adaptable framework, ensuring that AI in Cybersecurity programs remain dynamic, impactful, and aligned with the future needs of the industry.

In conclusion, this strategic approach not only prepares students for high-demand careers in cybersecurity but also advances the broader mission of equity, diversity, and innovation in STEM education. Through interdisciplinary collaboration, continuous curriculum enhancement, and strategic partnerships, HBCUs can play a definitive role in shaping the next generation of AI-driven cybersecurity professionals.

## REFERENCES


[1] D. V. V. Vegesna, "Enhancing cyber resilience by integrating ai-driven threat detection and mitigation strategies," *Transactions on Latest Trends in Artificial Intelligence*, vol. 4, no. 4, 2023. [Online]. Available: https://ijsdcs.com/index.php/TLAI/article/view/396

[2] M. Schmitt, "Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (ai)-enabled malware and intrusion detection," *Journal of Industrial Information Integration*, vol. 36, p. 100520, 2023. [Online]. Available: https://doi.org/10.1016/j.jii.2023.100520

[3] A. Anandita Iyer and K. S. Umadevi, "Role of ai and its impact on the development of cyber security applications," *Artificial Intelligence and Cyber Security in Industry 4.0*, p. 23–46, 2023. [Online]. Available: https://doi.org/10.1007/978-981-99-2115-7_2

[4] A. R. Sinha, K. Singla, and T. M. Victor, "Artificial intelligence and machine learning for cybersecurity applications and challenges," *Advances in Information Security, Privacy, and Ethics*, p. 109–146, Nov 2023. [Online]. Available: https://doi.org/10.4018/978-1-6684-9317-5.ch007

[5] S. M. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," in *Proceedings of the 31st International Conference on Neural Information Processing Systems*, ser. NIPS'17. Red Hook, NY, USA: Curran Associates Inc., 2017, p. 4768–4777. [Online]. Available: https://dl.acm.org/doi/10.5555/3295222.3295230

[6] M. T. Ribeiro, S. Singh, and C. Guestrin, "why should i trust you?" explaining the predictions of any classifier," in *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining*, 2016, pp. 1135–1144. [Online]. Available: https://doi.org/10.1145/2939672.2939778

[7] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial networks," *Commun. ACM*, vol. 63, no. 11, p. 139–144, oct 2020. [Online]. Available: https://doi.org/10.1145/3422622

[8] W. Hu and Y. Tan, "Generating adversarial malware examples for black-box attacks based on gan," in *International Conference on Data Mining and Big Data*. Springer, 2022, pp. 409–423. [Online]. Available: https://doi.org/10.1007/978-981-19-8991-9_29

[9] S. Laato, A. Farooq, H. Tenhunen, T. Pitkamaki, A. Hakkala, and A. Airola, "Ai in cybersecurity education - a systematic literature review of studies on cybersecurity moocs," in *2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT)*, 2020, pp. 6–10. [Online]. Available: https://doi.org/10.1109/ICALT49669.2020.00009

[10] J. Wei-Kocsis, M. Sabounchi, B. Yang, and T. Zhang, "Cybersecurity education in the age of artificial intelligence: A novel proactive and collaborative learning paradigm," in *2022 IEEE Frontiers in Education Conference (FIE)*, 2022, pp. 1–5. [Online]. Available: https://doi.org/10.1109/FIE56618.2022.9962643

[11] B. Alomar, Z. Trabelsi, T. Qayyum, and M. M. A. Parambil, "Ai and network security curricula: Minding the gap," in *2024 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 2024, pp. 1–7. [Online]. Available: https://doi.org/10.1109/EDUCON60312.2024.10578588

[12] C. Molnar, "Interpretable machine learning: a guide for making black box models explainable. 2019," URL *https://christophm.github.io/interpretable-ml-book*, 2019. [Online]. Available: https://doi.org/10.1007/978-981-99-2115-7_2

[13] S. Hooker, D. Erhan, P.-J. Kindermans, and B. Kim, "A benchmark for interpretability methods in deep neural networks," *Advances in neural information processing systems*, vol. 32, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID:202782699

[14] A. Shrikumar, P. Greenside, and A. Kundaje, "Learning important features through propagating activation differences," in *International conference on machine learning*. PMLR, 2017, pp. 3145–3153. [Online]. Available: https://api.semanticscholar.org/CorpusID:3385018

[15] W. Song, X. Li, S. Afroz, D. Garg, D. Kuznetsov, and H. Yin, "Mab-malware: A reinforcement learning framework for attacking static malware classifiers," *arXiv preprint arXiv:2003.03100*, 2020. [Online]. Available: https://doi.org/10.1145/3488932.3497768

[16] G. W. Romney, J. Guymon, M. D. Romney, and D. A. Carlson, "Curriculum for hands-on artificial intelligence cybersecurity," in *2019 18th International Conference on Information Technology Based Higher Education and Training (ITHET)*, 2019, pp. 1–8. [Online]. Available: https://doi.org/10.1109/ITHET46829.2019.8937373

[17] M. Lourens, A. P. Dabral, D. Gangodkar, N. Rathour, C. N. Tida, and A. Chadha, "Integration of ai with the cybersecurity: A detailed systematic review with the practical issues and challenges," in *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, 2022, pp. 1290–1295. [Online]. Available: https://doi.org/10.1109/IC3I56241.2022.10073040

[18] G. W. Romney, J. Guymon, M. D. Romney, and D. A. Carlson, "Curriculum for hands-on artificial intelligence cybersecurity," in *2019 18th International Conference on Information Technology Based Higher Education and Training (ITHET)*. IEEE, 2019, pp. 1–8. [Online]. Available: https://doi.org/10.1109/ITHET46829.2019.8937373

[19] T. Crick, J. H. Davenport, P. Hanna, A. Irons, and T. Prickett, "Overcoming the challenges of teaching cybersecurity in uk computer science degree programmes," in *2020 IEEE Frontiers in Education Conference (FIE)*, 2020, pp. 1–9. [Online]. Available: https://doi.org/10.1109/FIE44824.2020.9274033

[20] W. Nelson, K. Gosha, L. Haynes, A. Johnson, and N. Gilbert, "A hbcu program strategy for broadening participation in computing through local collaboration to increase chip-related professions," in *2024 Black Issues in Computing Education (BICE)*. Los Alamitos, CA, USA: IEEE Computer Society, feb 2024, pp. 21–26. [Online]. Available: https://doi.org/10.1109/BICE60192.2024.00012

[21] F. Farahmand, "Integrating cybersecurity and artificial intelligence research in engineering and computer science education," *IEEE Security Privacy*, vol. 19, no. 6, pp. 104–110, 2021. [Online]. Available: https://doi.org/10.1109/MSEC.2021.3103460

[22] E. Dillon, B. Williams, A. Ajayi, Z. Bright, Q. Kimble-Brown, C. Rogers, M. Lewis, J. Esema, B. Clinkscale, and K. L. Williams, "Exposing early cs majors to coding interview practices: An hbcu case study," in *2021 Conference on Research in Equitable and Sustained Participation in Engineering, Computing, and Technology (RESPECT)*, 2021, pp. 1–4. [Online]. Available: https://doi.org/10.1109/RESPECT51740.2021.9620557

[23] J. E. DeBello, E. Troja, and L. M. Truong, "A framework for infusing cybersecurity programs with real-world artificial intelligence education," in *2023 IEEE Global Engineering Education Conference (EDUCON)*, 2023, pp. 1–5. [Online]. Available: https://doi.org/10.1109/EDUCON54358.2023.10125138

[24] S. Rafiq, F. Kamran, and A. Afzal, "Investigating the benefits and challenges of interdisciplinary education in higher education settings," *JOURNAL OF SOCIAL RESEARCH DEVELOPMENT*, vol. 5, no. 1, p. 87–100, Mar. 2024. [Online]. Available: https://doi.org/10.53664/JSRD/05-01-2024-08-87-100

[25] C. Sample, S. M. Loo, C. Justice, E. Taylor, and C. Hampton, "Cyber-informed: Bridging cybersecurity and other disciplines," in *European Conference on Cyber Warfare and Security*, 2020. [Online]. Available: https://www.proquest.com/docview/2453791089

[26] C. Xin and B. K. Payne, "Special issue on interdisciplinary cybersecurity research: A critical high-impact practice in cybersecurity education," *OUR Journal: ODU Undergraduate Research Journal*, vol. 7, no. 1, p. 1, 2020. [Online]. Available: https://doi.org/10.25778/cs5t-y658

[27] X. Du, S. Alghowinem, M. Taylor, K. Darling, and C. Breazeal, "Innovating ai leadership education," in *2023 IEEE Frontiers in Education Conference (FIE)*. IEEE, 2023, pp. 1–8. [Online]. Available: https://doi.org/10.1109/FIE58773.2023.10343238

[28] R. G. Klaassen, "Interdisciplinary education: a case study," *European Journal of Engineering Education*, vol. 43, no. 6, pp. 842–859, 2018. [Online]. Available: https://doi.org/10.1080/03043797.2018.1442417

[29] T. Diphoorn, B. M. Leyh, S. C. Knittel, M. Huysmans, and M. Van Goch, "Traveling concepts in the classroom: Experiences in interdisciplinary education," *Journal of Interdisciplinary Studies in Education*, vol. 12, no. SI, pp. 1–14, 2023. [Online]. Available: https://doi.org/10.4337/9781035317967.ch131