Alignment of AI Knowledge Units and Cybersecurity Competencies for PUPR's Programs of Study

Author: Roberto L. Vivas Gotay
Advisor: Dr. Alfredo Cruz
Polytechnic University of Puerto Rico (Master in Computer Science)

Abstract

The rapid integration of artificial intelligence into cybersecurity has increased the need for clear, curriculum-level alignment with national cybersecurity education frameworks. This master's project presents a structured alignment of Artificial Intelligence in Cybersecurity knowledge units with the proposed Master of Science in Computer Science curriculum at the Polytechnic University of Puerto Rico. Rather than introducing new content, the study analyzes existing and planned graduate courses to identify embedded AI-enabled cybersecurity concepts and formally document them for accreditation and program evaluation. In parallel, cybersecurity competency statements were developed and aligned with nationally recognized workforce frameworks to support workforce relevance. The results show that a curriculum-first alignment strategy can satisfy Artificial Intelligence in Cybersecurity program expectations while preserving existing course structures, offering a replicable model for integrating AI into graduate cybersecurity education.

Introduction

The increasing adoption of artificial intelligence (AI) across modern cybersecurity operations has introduced new challenges for higher education institutions tasked with preparing graduates for an evolving threat landscape. AI techniques are now routinely applied to malware detection, intrusion analysis, automated incident response, and security analytics, requiring cybersecurity professionals to possess not only traditional defensive skills but also foundational knowledge of AI concepts and their ethical, operational, and security implications. As a result, academic programs must ensure that their curricula remain aligned with national cybersecurity education standards while also incorporating emerging AI-related competencies.

In response to these developments, federal and academic initiatives such as the Artificial Intelligence Cybersecurity (AICyber) framework and the National Centers of Academic Excellence in Cyber Defense (CAE-CD) program have emphasized the importance of formally documenting knowledge units, learning outcomes, and competencies that reflect both cybersecurity fundamentals and AI-enabled security practices [1]. However, integrating these frameworks into existing graduate curricula presents practical challenges. Many programs already contain relevant technical content but lack explicit alignment artifacts that demonstrate compliance with accreditation and workforce development expectations.

This master's degree project addresses this gap by structuring the alignment of AICyber knowledge units with the planned graduate curriculum of the Polytechnic University of Puerto Rico [2]. Additionally, selected course-level competencies are mapped to CAE-CD cybersecurity knowledge units to support institutional accreditation efforts. Rather than proposing new courses or redesigning existing ones, this work focuses on identifying how current and planned coursework already supports AI-relevant cybersecurity concepts and documenting those relationships in a manner consistent with CAE-CD and AICyber guidance.

By adopting a curriculum-first and competency-driven alignment approach, this project demonstrates how graduate programs can incorporate AI considerations into cybersecurity education without disrupting established academic structures. The outcomes of this study provide a practical framework for educational institutions seeking to strengthen their alignment with national cybersecurity and AI education initiatives while maintaining program coherence and academic rigor.

Methodology

This master's project follows a structured, artifact-driven alignment methodology designed to map graduate-level cybersecurity coursework to Artificial Intelligence Cybersecurity (AICyber) knowledge units and CAE-CD cybersecurity requirements. The methodology emphasizes documentation, traceability, and validation, rather than curriculum redesign, consistent with CAE-CD documentation and evaluation practices [3]. All alignment decisions are grounded in existing course syllabi, learning outcomes, topical coverage, and formally defined competency statements developed as part of this project.

Figure 1 provides a high-level overview of the alignment workflow employed in this study, illustrating the progression from curriculum artifact collection to final knowledge unit and competency validation.

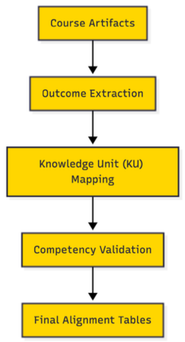

Figure 1: NSL – KDD Correlation Matrix

The primary data sources for this study consist of official graduate course documentation from the Master of Computer Science program at the Polytechnic University of Puerto Rico, including the proposed curriculum structure for the Area of Interest in Artificial Intelligence in Cybersecurity (AICyber) [2], [4]. These sources include course syllabi, catalog descriptions, learning outcomes, topical breakdowns, and assessment expectations. In addition, this project incorporates formally developed competency statements for selected courses, structured according to workforce-aligned templates. The scope of analysis includes cybersecurity, artificial intelligence, and AI-enabled cybersecurity courses relevant to AICyber and CAE-CD alignment. Courses without direct relevance to these domains were excluded to maintain analytical focus.

The alignment process was conducted in three successive layers: Knowledge Unit identification, course-level mapping, and program-level validation.

First, AICyber knowledge units were categorized into Cyber Foundational, AI Foundational, Core, and Optional groups, consistent with program-of-study requirements [5-6]. Each graduate course was reviewed to identify explicit and implicit coverage of AICyber knowledge units as defined in the AICyber knowledge unit documentation [6].

Second, course-level mappings were documented in detailed alignment matrices, associating each course with one or more AICyber knowledge units. This process resulted in a comprehensive mapping artifact that captures both breadth and depth of coverage across the curriculum.

Figure 2 illustrates the distribution of AICyber cyber foundational knowledge unit coverage across the graduate curriculum.

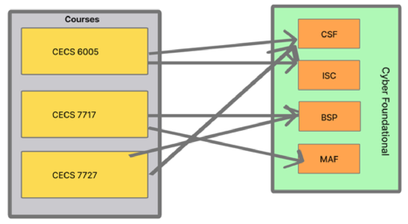

Figure 2: Final Alignment of Cyber Foundational KUs

The final phase of the methodology involved validating the completeness of alignment at the program level. Using the compiled course mappings, master alignment tables were constructed to evaluate whether the program satisfies AICyber program-of-study requirements, including minimum coverage of foundational, core, and optional knowledge units.

When multiple courses are aligned to the same knowledge unit, a row dominance principle was applied to identify primary contributors and reduce redundancy. This resulted in alternative final alignment configurations, each demonstrating compliance while highlighting different instructional emphases.\

Figure 3 visualizes the step-by-step process of classifying and validating portions of the Row Dominance Validation Process.

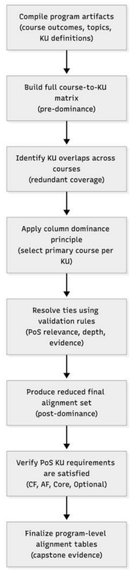

Figure 3: Row Dominance Validation Process

Results and Discussion

The finalized alignment confirms that the Master of Computer Science curriculum with a specialization in Artificial Intelligence in Cybersecurity satisfies all required AICyber program-of-study knowledge unit categories [6]. Using the structured knowledge unit mapping process and subsequent program-level validation, the curriculum demonstrates coverage of Cyber Foundational, AI Foundational, Core, and Optional AICyber knowledge units. The results of this study demonstrate that a curriculum-first alignment strategy can effectively integrate artificial intelligence considerations into graduate cybersecurity education without requiring structural changes to existing courses. Figure 4 shows the AI Foundational KUs aligned with the graduate courses.

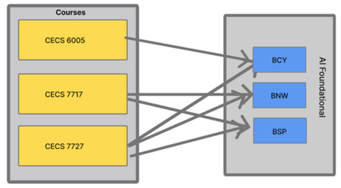

Figure 4: Final Alignment of AI Foundational KUs

Moreover, with regards to the core and optional KUs, Figure 5 shows that the graduate courses do fulfill also both core and optional KUs.

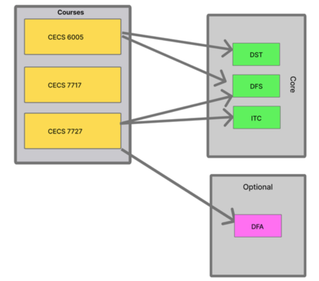

Figure 5: Final Alignment of Core and Optional KUs

Conclusions and Future Work

The results show that the program satisfies all required AICyber knowledge unit categories through documented course coverage. The row dominance principle reduced redundancy and clarified primary course contributions, strengthening accreditation alignment, while cybersecurity competencies aligned with the NICE Framework and the Department of Defense Cyber Workforce Framework (DCWF) demonstrated workforce relevance. Future work will extend this framework to additional institutions.

Acknowledgements

This material is based upon work supported by Dr. Alfredo Cruz. I want to sincerely thank him for his support and guidance throughout this project.

References

[1] Towson University, "NSA CAE AI Workshop – Artificial Intelligence and Cybersecurity Education," Mar. 2024. [Online]. Available: https://wp.towson.edu/secured-lab/nsa-cae-ai-workshop-march-2024/. [Accessed: Feb. 3, 2026].

[2] Polytechnic University of Puerto Rico, "Master of Computer Science Program," 2025. [Online]. Available: https://pupr.edu/master-computer-science/. [Accessed: Feb. 3, 2026].

[3] National Centers of Academic Excellence in Cybersecurity, "CAE-CD Document Library," 2025. [Online]. Available: https://www.cyber.mil/ncae-c/document-library. [Accessed: Feb. 3, 2026].

[4] Polytechnic University of Puerto Rico, "Proposed Master of Science in Computer Science Curriculum with Area of Interest in Artificial Intelligence in Cybersecurity (AICyber)," Graduate School curriculum flowchart, 2025.

[5] National Centers of Academic Excellence in Cybersecurity, "Artificial Intelligence and Cybersecurity Curriculum Guidance," unpublished document, 2024. [Online]. Available: https://docs.google.com/document/d/1K5DSnXWfrJilXuMTB5n8UOcSfLr1HbDx. [Accessed: Feb. 3, 2026].

[6] National Centers of Academic Excellence in Cybersecurity, "Cyber + AI Knowledge Units (AICyber)," unclassified report, 2024. [Online]. Available: https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cyber_ai_kus_stoneman.pdf. [Accessed: Feb. 3, 2026].