

Article

Designing SecureAI Curriculum for National Security Needs: The Illinois Tech Program of Study

Maurice Dawson ^{1,*}, Ahmed Ben Ayed ², Samson Quaye ¹ and Abdul Hadi Khan ¹

¹ Center for Cybersecurity and Forensic Education (C²SAFE), Illinois Institute of Technology, Chicago, IL 60616, USA; squaye@hawk.illinoistech.edu (S.Q.); akhan172@hawk.illinoistech.edu (A.H.K.)

² School of Engineering & Technology, National University, San Diego, CA 92123, USA; aayed@nu.edu

* Correspondence: mdawson2@illinoistech.edu

Abstract

Artificial Intelligence is increasingly embedded in national security, defense, and critical infrastructure systems, yet the security of these systems remains insufficiently addressed in traditional cybersecurity education. National initiatives led by the National Security Agency and the National Science Foundation have identified the Security of Artificial Intelligence (SecureAI) as a distinct educational priority supported by formal knowledge units and program validation requirements. Concurrently, workforce data and federal reporting reveal persistent shortages of qualified cybersecurity professionals, particularly in defense and government sectors. This paper presents Illinois Institute of Technology as a case study in the design of a SecureAI applied concentration aligned with NSA-style knowledge units and Center of Academic Excellence principles. The paper demonstrates how a four-course SecureAI program, anchored by a shared undergraduate and graduate cybersecurity foundation, addresses emerging AI security risks while strengthening the national cybersecurity workforce pipeline.

Keywords: SecureAI education; cybersecurity curriculum design; national security workforce; artificial intelligence security; Centers of Academic Excellence (CAE)

1. Introduction

Artificial intelligence (AI) systems increasingly support mission-critical functions across defense, government, and critical infrastructure. As these systems move into operational decision-making and automation, they introduce security risks that differ in important ways from those associated with traditional information systems. Attacks may target training data, model parameters, inference behavior, deployment environments, or post-deployment use, and can remain difficult to detect using conventional security controls. These risks are increasingly documented in national AI risk guidance, which emphasizes lifecycle-oriented threat exposure and the need for governance and assurance mechanisms in addition to technical controls ([National Institute of Standards and Technology, 2023](#)).

Despite the growing reliance on AI in high-stakes environments, cybersecurity education has been comparatively slow to treat the security of AI systems as a distinct competency area. Many curricula emphasize the use of AI techniques to enhance cybersecurity operations, yet provide limited structured coverage of threats to AI systems themselves, including adversarial manipulation, model integrity compromise, and AI supply chain risk.

In response, national stakeholders have begun to formalize SecureAI as a discrete educational priority. Guidance and validation expectations associated with national cybersecurity education initiatives emphasize the need for programs that can demonstrate



Academic Editor: Chris Campbell

Received: 7 January 2026

Revised: 6 February 2026

Accepted: 9 February 2026

Published: 13 February 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\) license](#).

structured coverage of SecureAI knowledge and skills aligned with workforce requirements (CyberAI Working Group, 2024; National Centers of Academic Excellence in Cybersecurity, 2024; National Security Agency, n.d.).

This paper addresses that gap by presenting Illinois Institute of Technology (IIT) as a case study in SecureAI program development. Specifically, the paper describes the design of a four-course SecureAI applied concentration embedded within existing undergraduate and graduate programs, organized to align with national knowledge units and to support workforce readiness in defense-adjacent and other regulated sectors. By documenting the program structure, shared foundational course model, and knowledge-unit alignment approach, this study contributes an example of how SecureAI can be integrated into established cybersecurity curricula while maintaining academic rigor and applied relevance (Burley et al., 2018; Yin, 2018).

2. Materials and Methods

2.1. Research Design

This study adopts a descriptive curriculum design case study approach to examine the development and structure of a SecureAI applied concentration at Illinois Institute of Technology. Case study methods are commonly used in education research to document, analyze, and contextualize curriculum innovations within real institutional settings, particularly when the objective is to describe design decisions, alignment processes, and educational frameworks rather than to test causal hypotheses (Clear et al., 2018; Yin, 2018). The focus of this study is on curriculum structure, knowledge unit alignment, and workforce relevance, positioning the SecureAI concentration as an illustrative example of how SecureAI education can be integrated into an existing cybersecurity program. The analytic focus of this study is on curriculum structure, Knowledge Unit alignment, and program-level coherence rather than on empirical evaluation of learning outcomes. Design objectives include demonstrating traceability between SecureAI Knowledge Units, course content, and assessed artifacts, and documenting how SecureAI competencies are scaffolded across a four-course applied concentration.

2.2. Data Sources

The analysis draws on multiple documentary data sources associated with the SecureAI concentration. These sources include official course catalog descriptions, draft and approved syllabi, SecureAI Knowledge Unit (KU) mapping documents, and program-level design materials developed within the Center for Cybersecurity and Forensics Education (CSAFE) at Illinois Institute of Technology. In addition, assessment artifacts referenced in this study, such as threat modeling assignments, secure AI architecture designs, and AI-focused risk analysis deliverables, are used to illustrate the applied learning emphasis of the curriculum. All data sources were institutional documents generated as part of program design and review processes rather than student-level records, and no personally identifiable student data were used in this study.

2.3. Analysis Approach

The curriculum analysis was conducted through structured document analysis and mapping. Course content and learning objectives were examined and mapped against SecureAI Knowledge Units as defined in national CyberAI guidance (CyberAI Working Group, 2024; National Centers of Academic Excellence in Cybersecurity, 2024). This mapping process was used to identify coverage across foundational cybersecurity competencies, AI foundations, SecureAI core technical topics, and AI risk management and governance.

In parallel, curriculum components were examined for alignment with nationally recognized workforce frameworks, including NICE-aligned role categories and defense-oriented cyber workforce expectations (Department of Defense, 2023; DoD Workforce Innovation Directorate, n.d.; Petersen et al., 2020). This role-based perspective supports evaluation of workforce relevance without making claims about employment outcomes. The analysis emphasizes traceability between courses, SecureAI Knowledge Units, and representative workforce roles rather than quantitative measures of effectiveness.

2.4. Validation and Review Considerations

To support internal consistency and relevance, the SecureAI curriculum design was informed by faculty expertise in cybersecurity, AI systems, and applied security education. Program documentation and KU mappings were reviewed iteratively during the design process to ensure coherence across undergraduate and graduate offerings and to minimize unnecessary duplication. This approach is consistent with recommendations in cybersecurity education research that emphasize iterative curriculum review and framework-based alignment as indicators of program rigor (Burley et al., 2018; Ngambeki et al., 2021).

2.5. Scope and Limitations

This study is limited to a descriptive analysis of curriculum design and alignment. It does not evaluate student learning outcomes quantitatively, measure employment placement, or assess long-term workforce impact. Longitudinal evaluation of SecureAI educational outcomes, such as analysis of student artifacts, enrollment trends, employer feedback, and graduate career trajectories is identified as an important direction for future research.

3. Workforce Demand and National Security Context

Cybersecurity workforce shortages in the United States remain persistent across sectors and increasingly constrain national security readiness. CyberSeek's latest national update reports 514,359 cybersecurity job listings over the past 12 months, while the overall supply-demand ratio is 74%, indicating that the available workforce falls short of employer demand (CyberSeek, 2025b; NIST, 2025). This challenge is especially visible in the defense ecosystem. The U.S. Department of Defense has reported a shortage of over 20,000 cyber professionals, which has increased reliance on retraining pipelines and academic partnerships to reduce mission risk (DoD CIO, 2025).

These pressures also reflect a broader global crisis. The (ISC)² 2024 Cybersecurity Workforce Study estimates a global workforce gap of approximately 4.8 million professionals, reinforcing that the pipeline problem is systemic rather than localized (ISC2, 2024). Prior scholarship suggests that the response cannot be limited to expanding conventional cybersecurity coursework. Dawson argues that national cybersecurity education must evolve beyond narrow defensive skill-building toward adversarial reasoning and operationally realistic preparation (Dawson, 2020, 2024). Related work further highlights that workforce gaps are particularly consequential in critical infrastructure settings, where cyber incidents may cascade into physical and societal impacts (Dawson et al., 2021).

At the same time, AI is reshaping both cyber operations and the cybersecurity labor market. CyberSeek's 2025 reporting emphasizes an expanding intersection between cybersecurity and AI skills, with postings increasingly requesting AI/ML exposure (CyberSeek, 2025b). Yet SecureAI requires competencies not consistently covered in traditional curricula, such as adversarial machine learning, model integrity, secure deployment, and AI governance. Dawson and Szakonyi emphasize that awareness of AI security risks remains limited among developers and end users, while Dawson and Omotoye illustrate the growing need for interdisciplinary models that integrate security with emerging data-driven

systems (Dawson & Omotoye, 2024; Dawson & Szakonyi, 2020). Together, these trends support the case that SecureAI education is both a workforce necessity and a national security imperative.

State of Illinois Supply vs. Demand

CyberSeek’s Supply/Demand Heat Map indicates that Illinois remains a “tight” labor market for cybersecurity, with demand concentrated in a small number of metropolitan zones (CyberSeek, 2025a). The Chicago–Naperville–Elgin region dominates statewide activity, with additional hubs linked to government services, finance/insurance, and defense-adjacent operations. This geographic concentration is captured in Figure 1 and reflected in the statewide metrics summarized in Tables 1 and 2. Importantly, the same AI-driven shift visible nationally is also emerging locally, reinforcing the need for SecureAI-aligned educational pathways that prepare graduates for AI-enabled security environments (CyberSeek, 2025b).

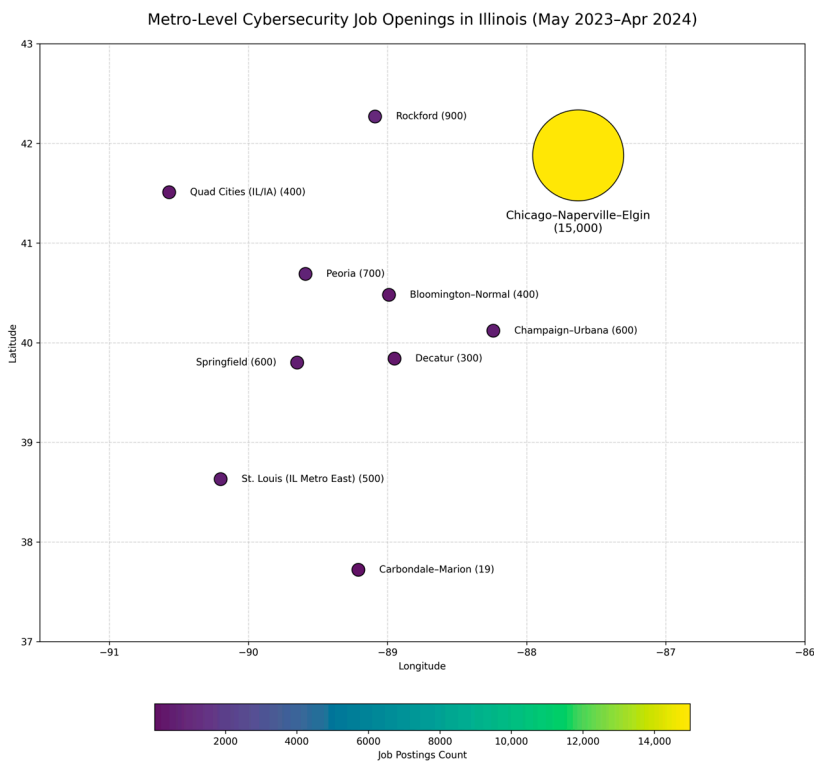


Figure 1. Illinois metro visualization of cybersecurity demand (illustrative heat map). Note: Visualization created by the authors based on CyberSeek Supply/Demand Heat Map data (CyberSeek, 2025a).

Table 1. Illinois cybersecurity workforce overview (CyberSeek 2024–2025).

Metric	Illinois Data	Comparison/Context
Total Online Job Openings	~21,450	Illinois is among the top 10 states for job volume.
Total Employed Workforce	~44,800	Professionals currently working in cyber roles.
Supply/Demand Ratio	0.72	Only 72 workers are available for every 100 openings.
Location Quotient (LQ)	1.05	Slightly higher concentration of cyber jobs than the US avg.
Public Sector Openings	~1200	Includes State, Local, and Federal roles in IL.

Table 2. Top cybersecurity job openings in Illinois by title.

Rank	Job Title	Estimated Annual Openings
1	Cybersecurity Engineer	5800+
2	Cybersecurity Analyst	4200+
3	Cybersecurity Manager	2100+
4	Software Development (Security focused)	1900+
5	Systems Engineer	1400+

Illinois workforce demand is also shifting toward AI-related competencies. CyberSeek's 2025 reporting suggests that roughly one in ten cybersecurity job postings in Illinois references AI or machine learning skills, signaling growing employer demand for talent that can operate at the cybersecurity, AI intersection (CyberSeek, 2025b). This local signal strengthens the rationale for SecureAI-aligned education, because AI-enabled systems introduce distinct threat models, such as adversarial manipulation and model integrity risks, that are not consistently addressed in traditional cybersecurity coursework.

4. SecureAI as a Distinct Educational Domain

4.1. Distinguishing SecureAI from AI for Cybersecurity

SecureAI differs fundamentally from the application of artificial intelligence to cybersecurity tasks. Much of the existing literature and practice emphasizes AI for cybersecurity, where machine learning supports intrusion detection, malware classification, anomaly detection, and automated response. In contrast, SecureAI focuses on the security of AI systems themselves, treating models, training data, pipelines, and inference interfaces as protected assets that must be defended across the AI lifecycle (MITRE, n.d.; Vassilev et al., 2025).

This distinction is not merely semantic. AI-enabled systems introduce attack surfaces that do not align cleanly with traditional network- and host-based security assumptions. Research on adversarial examples demonstrates that models can be induced to misclassify inputs through carefully crafted perturbations, even when changes are small or operationally plausible (Goodfellow et al., 2015; Szegedy et al., 2014). Subsequent work has shown that attacks can remain effective in black-box settings through transferability and substitute models, highlighting the practical relevance of inference-time manipulation (Papernot et al., 2016, 2017). These attack modes require students to reason about model behavior and threat models that are typically outside conventional cybersecurity coursework.

SecureAI also encompasses training-time compromise, where attackers manipulate datasets or training workflows to degrade or control model behavior. Poisoning research demonstrates that an adversary can inject or shape training points to increase error or induce targeted failures, even against widely deployed learning methods (Biggio et al., 2012; Jagielski et al., 2018). Taken together, these findings support treating SecureAI as a distinct domain, because the defenses and competencies required extend beyond conventional cyber controls and demand integrated knowledge of both security engineering and machine learning.

4.2. SecureAI Threat Landscape and Technical Scope

The SecureAI threat landscape expands across the full AI lifecycle, data acquisition, training, evaluation, deployment, and operation. NIST's adversarial machine learning taxonomy emphasizes lifecycle stages, attacker goals, attacker knowledge, and the interaction between ML-specific vulnerabilities and broader system weaknesses (Vassilev et al., 2025). MITRE ATLAS similarly organizes real-world and demonstrated adversary tactics against AI-enabled systems, reinforcing that AI components and workflows require explicit threat modeling (MITRE, n.d.).

Beyond evasion and poisoning, SecureAI includes privacy and intellectual property threats that arise from the exposure of model interfaces. Membership inference attacks show that adversaries can infer whether a specific record was included in training, creating privacy risks for sensitive domains such as healthcare and national security (Shokri et al., 2017). Model inversion attacks demonstrate that confidence scores and prediction interfaces can leak sensitive attributes or approximate training data characteristics (Fredrikson et al., 2015). Model extraction attacks show that a deployed prediction API can be queried to reconstruct a high-fidelity copy of a target model, undermining intellectual property protections and enabling downstream evasion (Tramèr et al., 2016). These risks directly motivate secure deployment practices, access control, monitoring, and interface hardening.

Generative AI and foundation models add application-level failure modes that are now widely recognized in security practice. Community-driven risk taxonomies for large language model (LLM) applications highlight prompt injection, insecure output handling, training data poisoning, and supply-chain vulnerabilities as recurring classes of issues in deployed systems (OWASP, 2025). For education, the implication is that SecureAI instruction must extend beyond “robustness” to include secure architecture, model serving security, monitoring and incident response, and governance controls for AI-enabled applications.

Recent research further demonstrates that LLM applications introduce distinct attack surfaces related to prompt injection, retrieval-augmented generation (RAG) data poisoning, and insecure orchestration of external tools, which can lead to unauthorized actions or leakage of sensitive information (Greshake et al., 2023; Liu et al., 2024). Additional studies on secure model serving show that inference APIs and deployment pipelines remain vulnerable to extraction, abuse, and supply-chain compromise unless explicitly protected through architectural controls and monitoring mechanisms (Carlini et al., 2023; Kumar et al., 2023; Zhang et al., 2022).

4.3. SecureAI Knowledge Units and Domain Structure

National SecureAI frameworks increasingly formalize this domain through structured competency expectations that span cybersecurity foundations, AI foundations, SecureAI technical skills, and AI risk management. From a curriculum standpoint, these frameworks help ensure that SecureAI is taught as a coherent learning progression rather than a collection of disconnected topics. NIST’s AI risk framing reinforces that trustworthy AI requires attention to governance and operational controls in addition to technical mitigations (National Institute of Standards and Technology, 2023; Vassilev et al., 2025). MITRE ATLAS provides an operationally grounded mapping of AI attack techniques that can support course learning outcomes and assessment artifacts (MITRE, n.d.). OWASP’s LLM application risks can be used to structure applied secure-by-design projects for generative AI systems (OWASP, 2025).

To support academic rigor, a SecureAI domain structure should clearly connect (a) lifecycle threats, (b) technical controls, and (c) organizational controls.

4.4. SecureAI as a Socio-Technical Educational Domain

SecureAI is inherently socio-technical. Effective protection of AI systems requires engineering controls, but also governance mechanisms, documentation practices, risk ownership, and policy alignment. The NIST AI Risk Management Framework treats AI risk as an organizational responsibility and emphasizes governance functions that shape how systems are designed, deployed, monitored, and retired (National Institute of Standards and Technology, 2023). This aligns with the reality that AI security failures can create downstream impacts beyond technical malfunction, privacy harms, operational disruption, safety hazards, and loss of public trust.

Accordingly, SecureAI education must train students to evaluate trade-offs among model performance, security, privacy, transparency, and governance constraints. This includes learning how to communicate AI system risk, justify mitigation choices, and integrate monitoring and incident response into AI deployment pipelines. Such socio-technical competence is difficult to develop through purely technical labs alone, reinforcing the need for a structured SecureAI pathway rather than a single elective module.

4.5. Implications for SecureAI Curriculum Design

Recognizing SecureAI as a distinct educational domain has direct implications for curriculum design. Programs should avoid treating AI security as a peripheral topic and instead provide structured learning pathways that progressively develop competencies across AI foundations, adversarial threat modeling, secure system engineering, and risk governance. A practical curriculum should teach students to (1) identify lifecycle threats using taxonomies, (2) implement and evaluate defenses using established methods from the adversarial ML literature, and (3) produce applied artifacts such as threat models, secure deployment designs, and risk registers aligned with organizational controls (MITRE, n.d.; National Institute of Standards and Technology, 2023; Vassilev et al., 2025).

This conceptual framing provides the foundation for the SecureAI program design and course mapping presented in the following sections.

5. SecureAI Knowledge Units and CAE Expectations

5.1. Role of Knowledge Units in SecureAI Curriculum Design

SecureAI KUs provide a standardized way to define what students should know and be able to do in order to secure AI-enabled systems. Within the CAE ecosystem, KUs function as competency “building blocks” that support consistent curriculum design, documentation, and assessment across institutions (National Centers of Academic Excellence in Cybersecurity, 2023; National Security Agency, n.d.). In the CyberAI context, KU-based design is especially important because SecureAI spans multiple disciplinary layers, cybersecurity, AI foundations, secure systems engineering, and governance, making it difficult to ensure coverage through ad hoc course topics alone (CyberAI Working Group, 2024). The CyberAI KU model structures SecureAI learning expectations around a coherent domain progression. At a minimum, SecureAI programs must demonstrate that students build (a) cybersecurity foundations, (b) AI foundations, (c) SecureAI core technical competencies, and (d) AI risk management and governance competencies, with sufficient depth to support applied work in high-risk settings (CyberAI Working Group, 2024; National Centers of Academic Excellence in Cybersecurity, 2024). This structure helps avoid a common curriculum failure mode in which AI security is treated as a “capstone-only” topic without the prerequisite knowledge required to reason about model behavior, lifecycle threats, and operational control requirements. Sufficiency of SecureAI Knowledge Unit coverage was determined through structured mapping of required CyberAI SecureAI Knowledge Units to course learning objectives and assessed artifacts, followed by program-level review to ensure cumulative coverage across the full four-course concentration.

5.2. CyberAI Programs of Study and SecureAI KU Expectations

The CyberAI Program of Study (PoS) validation requirements make KU coverage explicit and auditable. Rather than allowing institutions to claim SecureAI alignment through broad course descriptions, the PoS framework expects institutions to show traceability between KUs, course outcomes, and assessed student work products (National Centers of Academic Excellence in Cybersecurity, 2024). The PoS documentation further distinguishes SecureAI from AI-for-cybersecurity (AICyber), emphasizing that SecureAI focuses on securing AI

systems and infrastructure throughout the lifecycle, while AICyber emphasizes using AI to enhance traditional cybersecurity tasks (CyberAI Working Group, 2024). In practical terms, this validation logic pushes programs to do more than “cover topics.” It requires evidence that students can apply SecureAI competencies through artifacts such as threat models for AI systems, secure deployment designs, monitoring incident response plans for AI-enabled services, and risk and governance deliverables aligned with organizational controls (National Centers of Academic Excellence in Cybersecurity, 2024). This evidence-based orientation is consistent with CAE principles that prioritize demonstrable academic rigor and applied relevance (CAE Community, n.d.; National Security Agency, n.d.).

5.3. CAE Alignment, Traceability, and Assessment Expectations

CAE designation requirements emphasize curriculum alignment to defined KUs and the production of clear program documentation (National Centers of Academic Excellence in Cybersecurity, 2023; Dawson et al., 2018; Wang et al., 2019). Across CAE pathways, institutions are typically expected to provide curriculum maps that show where each KU is introduced, reinforced, and assessed, along with a program plan that ensures students can navigate KU coverage through a coherent academic pathway (National Centers of Academic Excellence in Cybersecurity, 2023). In effect, KU mapping becomes an accountability mechanism: it enables external reviewers to verify that SecureAI learning outcomes are systematically supported rather than depending on instructor discretion or elective availability. Because SecureAI spans both technical and socio-technical dimensions, KU mapping is most defensible when paired with assessment strategies that include both (a) technical demonstrations and (b) governance and risk artifacts. This is also where workforce alignment can be strengthened by connecting program outcomes to recognized cybersecurity work-role language. The NICE Workforce Framework provides a nationally recognized structure for describing cybersecurity work in terms of tasks, knowledge, and skills, and it is commonly used to justify how academic outcomes translate into workforce readiness (Petersen et al., 2020). For SecureAI, NICE alignment is useful not because it replaces SecureAI KUs, but because it helps situate SecureAI competencies within broader cybersecurity career pathways that institutions and employers already recognize (Petersen et al., 2020).

5.4. Continuous Improvement and Faculty Engagement

The CyberAI PoS validation process places strong emphasis on continuous improvement. Programs are expected to document review cycles, incorporate stakeholder feedback, and demonstrate responsiveness to evolving threats and technology changes (National Centers of Academic Excellence in Cybersecurity, 2024). This expectation is particularly important for SecureAI because the threat landscape and deployment patterns change faster than in many traditional cybersecurity domains. Continuous improvement mechanisms can include instructor working groups, periodic KU mapping reviews, employer/advisory input, and evidence-driven course updates based on assessment performance and student outcomes (CAE Community, n.d.; National Centers of Academic Excellence in Cybersecurity, 2024). Faculty engagement is similarly central. A KU-driven program assumes that instructors have sufficient expertise to deliver both AI and security content, and that the program has a process to maintain instructional quality as content evolves (National Centers of Academic Excellence in Cybersecurity, 2024; National Security Agency, n.d.).

5.5. Implications for the IIT SecureAI Concentration

For the IIT SecureAI concentration, the KU and PoS expectations imply two design obligations. First, the program must show systematic KU coverage across its four-course sequence, with explicit points where KUs are assessed through applied artifacts. Second, it must document program-level learning outcomes, course mapping traceability, and

a continuous improvement approach that demonstrates sustained alignment to CAE-style expectations and CyberAI PoS validation requirements (CyberAI Working Group, 2024; National Centers of Academic Excellence in Cybersecurity, 2024). These principles provide the basis for the course-to-KU mapping and assessment design presented in the subsequent sections.

6. Illinois Institute of Technology as a SecureAI Case Study

IIT provides an established institutional foundation for integrating SecureAI education within existing Information Technology and Management (ITM) programs. Rather than creating a standalone degree, IIT adopted a four-course applied concentration model embedded within its undergraduate and graduate curricula. This approach reflects a pragmatic strategy that leverages existing cybersecurity infrastructure while introducing SecureAI competencies in a structured and scalable manner.

Applied concentrations have been widely recognized in computing education as an effective mechanism for addressing emerging technical domains without fragmenting academic programs or delaying student progression (Clear et al., 2018; Mulder & Jansen, 2020). By embedding SecureAI within existing degree pathways, IIT enables students to build advanced competencies while maintaining alignment with established accreditation, advising, and workforce pipelines.

A defining feature of the SecureAI concentration is the use of a shared cybersecurity foundation course, delivered as ITMS 458 at the undergraduate level and ITMS 548 at the graduate level. Both courses are aligned in terms of core content, learning objectives, and SecureAI Knowledge Unit coverage. Differentiation between undergraduate and graduate delivery is achieved through assignment depth, analytical expectations, and assessment rigor rather than through divergent topic coverage. This shared-course model reflects a pedagogical approach commonly used in professional computing programs to support vertical integration while preserving academic standards (Biggs & Tang, 2011; Lister et al., 2016).

The cybersecurity technologies course serves as the technical baseline upon which SecureAI competencies are later developed. Course content addresses core security mechanisms and threat concepts, including malware and attack techniques, system and network vulnerabilities, defensive countermeasures, security protocols, cryptographic foundations, identity and authentication mechanisms, scanning and monitoring tools, firewalls, and the role of standards and professional organizations in cybersecurity practice. These topics align with foundational cybersecurity knowledge expected for advanced work in AI-enabled environments, where secure deployment and operational context are as critical as model-level defenses (Bishop, 2019; Scarfone & Mell, 2012).

An applied team-based project is a central component of course design. Students collaborate on a self-contained security project that emphasizes system integration, threat analysis, and practical implementation. Project-based learning has been shown to enhance student engagement and deepen conceptual understanding in cybersecurity education by requiring learners to apply theory to realistic scenarios and to reason about trade-offs under operational constraints (Burley et al., 2018; Logan & Clarkson, 2015). Importantly, the project structure allows for extension into follow-on coursework, supporting continuity across the SecureAI concentration and reinforcing lifecycle thinking.

Prerequisite coursework in networking, systems, and operating environments ensures that students enter the SecureAI pathway with sufficient technical maturity. This sequencing is consistent with research on curriculum scaffolding, which emphasizes the importance of establishing foundational mental models before introducing complex, interdisciplinary domains such as AI security (Shannon & Weaver, 2019; Sweller et al., 2011).

Taken together, the IIT SecureAI concentration illustrates how SecureAI education can be integrated into an existing cybersecurity curriculum without duplicating content or introducing parallel degree structures. The shared foundational course, combined with applied concentration design, provides a coherent entry point for subsequent SecureAI coursework while maintaining alignment with Knowledge Unit expectations and workforce-relevant skills. This case study therefore offers a transferable model for institutions seeking to incorporate SecureAI into established computing programs in a sustainable and academically rigorous manner.

7. SecureAI Program Design at Illinois Institute of Technology

7.1. Four-Course SecureAI Structure

The SecureAI applied concentration at Illinois Institute of Technology is structured as a four-course sequence designed to progressively develop competencies aligned with SecureAI Knowledge Units. The structure balances foundational preparation, technical depth, and governance-oriented understanding, while remaining embedded within existing undergraduate and graduate degree programs. Rather than isolating SecureAI into a single advanced course, the sequence distributes learning objectives across multiple courses to support scaffolding and reinforcement of key concepts. The four-course structure is summarized in Table 3, which outlines each course's role within the concentration and its availability at the undergraduate and graduate levels.

Table 3. SecureAI Applied Concentration Course Structure.

Course	Role in Program	Academic Level
ITMS 458/ITMS 548—Cyber Security Technologies	Cybersecurity foundation for SecureAI	Undergraduate/Graduate
ITMS 4XX/5XX—Foundations of Secure AI Systems	AI foundations and consolidated AI mathematics	Undergraduate/Graduate
ITMS 4XX/5XX—Secure AI Systems Engineering and Defense	SecureAI core technical defenses	Undergraduate/Graduate
ITMS 4XX/5XX—AI Risk Management and Governance	AI risk, policy, and governance	Undergraduate/Graduate

7.2. Shared Undergraduate and Graduate Cybersecurity Foundation

A defining feature of the SecureAI concentration is the use of a shared cybersecurity foundation course, offered as ITMS 458 at the undergraduate level and ITMS 548 at the graduate level. The two offerings are aligned in terms of content scope, learning objectives, and SecureAI Knowledge Unit coverage. Differentiation is achieved through the depth of analysis, complexity of assignments, and rigor of assessment, rather than through divergent subject matter. Undergraduate students primarily focus on application-oriented learning and skill development, emphasizing hands-on engagement with security technologies and operational scenarios. Graduate students engage with the same technical material but are expected to demonstrate deeper analytical reasoning, design justification, and consideration of enterprise-scale constraints. This shared-course model supports curriculum efficiency while maintaining academic rigor and has the additional benefit of reinforcing continuity across the SecureAI concentration.

7.3. SecureAI Knowledge Unit Coverage

SecureAI Knowledge Unit coverage across the four-course sequence is intentionally distributed to ensure both breadth and depth. Foundational KUs are addressed early in

the program, while SecureAI-specific technical and governance competencies are introduced and reinforced in later courses. This distribution supports cumulative learning and avoids overloading individual courses with disconnected objectives. Table 4 illustrates the alignment between SecureAI Knowledge Units and the courses in which they are primarily addressed. Table 4 summarizes the cumulative SecureAI Knowledge Unit coverage across the full four-course applied concentration, illustrating how competencies are progressively introduced and reinforced at the program level rather than mapped to individual courses in isolation.

Table 4. SecureAI Knowledge Unit to course mapping. The symbol ✓ indicates that the SecureAI Knowledge Unit is substantively covered and assessed in the corresponding course..

SecureAI Knowledge Unit	ITMS 458/548	Foundations of Secure AI	Secure AI Engineering	AI Risk & Governance
Cybersecurity Fundamentals	✓			
IT Systems Components	✓			
Basic Scripting & Programming	✓			
AI Foundations		✓		
AI Mathematics & Statistics		✓ (consolidated)		
AI System Lifecycle		✓	✓	
Adversarial Machine Learning			✓	
Model Integrity & Robustness			✓	
Secure Model Deployment			✓	
AI Monitoring & Incident Response			✓	
AI Supply Chain Risk			✓	
AIR—AI Risk Management				✓
AI Governance & Policy				✓

This mapping illustrates how SecureAI competencies are introduced progressively, moving from foundational knowledge toward applied defense and organizational risk management. The structure ensures that students encounter SecureAI threats and controls in both technical and socio-technical contexts.

8. Workforce Alignment and Career Pathways

A central design goal of the Illinois Tech SecureAI concentration is to strengthen workforce readiness by aligning curriculum outcomes with nationally recognized role and competency frameworks. In the United States, the National Initiative for Cybersecurity Education (NICE) Workforce Framework provides a common lexicon of cybersecurity work in terms of roles, tasks, and associated knowledge and skills, enabling clearer alignment between educational programs and workforce expectations (Petersen et al., 2020; National Initiative for Cybersecurity Education, 2017). This alignment principle is especially relevant for SecureAI because many organizations will source SecureAI talent through existing cybersecurity roles that are being extended with AI-specific security responsibilities rather than through fully distinct job families (MITRE, n.d.; National Institute of Standards and Technology, 2023).

At the federal level, workforce coding and qualification mechanisms also reinforce the value of role-based alignment. The Department of Defense (DoD), for example, formalizes cybersecurity workforce requirements through its Cyberspace Workforce Qualification and

Management Program and the DoD Cyber Workforce Framework, which are intended to ensure personnel filling cyber positions are qualified to meet mission needs ([Department of Defense, 2023](#); [DoD Workforce Innovation Directorate, n.d.](#)). In practice, these frameworks increase the importance of competency-based education that can demonstrate traceability from course outcomes to role expectations, particularly for defense-adjacent employment pathways.

Within this context, the SecureAI concentration is positioned to support multiple NICE-aligned role trajectories. Foundational cybersecurity competencies support roles such as cyber defense analysis and incident response, while SecureAI engineering content supports roles that require secure system design, testing, and operational hardening of AI-enabled components. The governance and risk course supports risk management-oriented roles, reflecting the broader view that AI security is not only a technical problem but also an organizational risk management responsibility ([National Institute of Standards and Technology, 2023](#)). MITRE ATLAS further reinforces this socio-technical reality by documenting adversary tactics and techniques against AI-enabled systems in ways that can inform defensive operations, testing, and monitoring practices relevant to both engineering and defensive teams ([MITRE, n.d.](#)).

To make this alignment explicit, Table 5 provides an example mapping from SecureAI concentration components to representative NICE work roles and common career pathways. This table is intended as a program-level alignment aid, consistent with prior education research showing that NICE-based course mapping can support curricular improvement and strengthen workforce relevance ([Ngambeki et al., 2021](#)).

Table 5. Example Workforce Role Alignment for the SecureAI Concentration (Illustrative).

SecureAI Concentration Component	Representative Workforce Role Targets (NICE-Aligned Examples)	Typical Employment Contexts
Cybersecurity foundation (ITMS 458/548)	Cyber Defense Analyst; Incident Responder; Cyber Defense Infrastructure Support	SOC/IR teams, government IT/security, regulated enterprise security
AI foundations & math (Foundations of Secure AI Systems)	Security-focused data/ML practitioner; security analyst supporting AI-enabled systems	AI-enabled security operations, security engineering teams collaborating with data/ML
SecureAI engineering & defense (Secure AI Systems Engineering and Defense)	Security engineer for AI-enabled systems; adversarial testing/red-teaming support; secure deployment engineering	Defense/IC contractors, critical infrastructure security engineering, security assurance teams
Risk management & governance (AI Risk Management and Governance)	Risk Management Specialist; governance/compliance roles supporting AI systems	Federal/state programs, healthcare/finance compliance, enterprise AI governance

This role-oriented framing clarifies that SecureAI education supports multiple pathways rather than a single “AI security job.” Early-career graduates may enter through established cyber defense roles and progressively assume SecureAI-specific responsibilities such as AI system threat modeling, adversarial testing, deployment hardening, and AI risk governance activities that align with national guidance emphasizing lifecycle risk management and trustworthiness ([National Institute of Standards and Technology, 2023](#)). The concentration therefore aims to expand employability across defense, government, critical infrastructure, and regulated industries by providing a structured foundation for secure AI deployment practices while maintaining compatibility with workforce frameworks widely used in public-sector hiring and qualification contexts ([Department of Defense, 2023](#); [Petersen et al., 2020](#)).

9. Program Validation and Continuous Improvement

Program validation and continuous improvement are essential components of SecureAI education, particularly given the rapid evolution of artificial intelligence technologies and associated threat landscapes. Within the National Centers of Academic Excellence in Cybersecurity (NCAE-C) ecosystem, CyberAI Programs of Study validation emphasizes the need for transparent documentation of KU coverage, evidence of faculty expertise, and mechanisms that support ongoing curriculum alignment with national workforce and security priorities ([National Centers of Academic Excellence in Cybersecurity, 2024](#); [National Security Agency, n.d.](#)).

The Illinois Tech SecureAI concentration is structured to support these expectations through explicit mapping between courses and SecureAI Knowledge Units, as presented in earlier sections. This mapping approach aligns with established best practices in cybersecurity and computing education, where course-to-framework traceability is used to demonstrate curriculum coherence and completeness rather than reliance on isolated course descriptions ([Burley et al., 2018](#); [Ngambeki et al., 2021](#)). Such traceability provides a foundation for periodic curriculum review and facilitates structured updates as SecureAI guidance evolves.

Assessment strategies within the SecureAI concentration emphasize applied learning artifacts that reflect real-world SecureAI practice. Rather than relying solely on traditional examinations, courses incorporate deliverables such as AI system threat models, adversarial risk analyses, secure deployment designs, and AI-focused risk registers. Prior education research indicates that artifact-based assessment supports deeper learning and better alignment with professional practice in cybersecurity and related applied domains ([Logan & Clarkson, 2015](#); [Mulder & Jansen, 2020](#)). In the SecureAI context, these artifacts also provide tangible evidence of student engagement with lifecycle-oriented AI security challenges. For example, SecureAI competencies are evaluated through applied artifacts such as AI system threat models, in which students identify lifecycle threats, justify mitigation strategies, and align controls with recognized SecureAI taxonomies.

Continuous improvement is further supported through periodic review of course content against emerging SecureAI frameworks and threat taxonomies, including updates to adversarial machine learning guidance and AI risk management practices. This approach reflects broader guidance from NIST and the CAE community, which emphasizes that cybersecurity and AI-related curricula must remain adaptive to maintain relevance in operational environments ([National Centers of Academic Excellence in Cybersecurity, 2024](#); [National Institute of Standards and Technology, 2023](#)). By grounding program evolution in nationally recognized frameworks rather than ad hoc updates, the SecureAI concentration supports sustained alignment with workforce needs and national security considerations.

Taken together, documented KU alignment, applied assessment artifacts, and structured review mechanisms provide a foundation for validating the SecureAI concentration as an academically rigorous and practice-oriented program of study. These elements position the program to respond effectively to changes in SecureAI guidance while maintaining consistency with established CAE-aligned educational principles.

10. Discussion

This case study illustrates how SecureAI education can be integrated into an existing cybersecurity curriculum in a way that is scalable and avoids unnecessary duplication. A key design decision is the use of a shared cybersecurity foundation course delivered at two academic levels (ITMS 458 for undergraduate students and ITMS 548 for graduate students). Although the course content and learning objectives remain aligned, differentiation occurs through assignment depth, analytical expectations, and assessment rigor. This structure

supports program efficiency while maintaining an appropriate level of academic challenge, which is consistent with established principles of constructive alignment and scaffolded learning in higher education (Biggs & Tang, 2011; Sweller et al., 2011).

Beyond the shared foundation, the four-course sequence reflects an intentional progression from cybersecurity fundamentals to AI foundations, SecureAI systems engineering, and organizational risk management. This sequencing reinforces the idea that SecureAI is not a single-topic specialization but a lifecycle-oriented domain requiring both technical and socio-technical competencies. Aligning the concentration to formal SecureAI Knowledge Units and CyberAI Programs of Study expectations provides a transparent basis for curriculum mapping and review, which is central to CAE-style curriculum practices (National Centers of Academic Excellence in Cybersecurity, 2024; National Security Agency, n.d.). The use of applied artifacts, such as threat models, secure AI architecture designs, and risk registers, further supports educational relevance by linking course assessment to outputs that resemble professional SecureAI practice (Burley et al., 2018; Logan & Clarkson, 2015).

The case study also suggests that SecureAI curriculum design can be made transferable across institutions by treating KU alignment as a design constraint rather than an after-the-fact documentation step. This approach may be particularly useful for institutions that already maintain CAE-aligned cybersecurity programs and wish to extend them to SecureAI without introducing a separate degree program. However, transferability depends on institutional factors such as faculty expertise, local program structures, and the availability of prerequisite coursework. As SecureAI guidance continues to evolve, curriculum models will need to remain adaptive, using nationally recognized frameworks to maintain coherence as new threats and deployment patterns emerge (MITRE, n.d.; National Institute of Standards and Technology, 2023).

Overall, the Illinois Tech SecureAI concentration demonstrates a practical model for expanding cybersecurity education into SecureAI through structured sequencing, shared foundational coursework, and documented KU alignment. This model provides a foundation that other CAE institutions can adapt when integrating SecureAI competencies into existing cybersecurity programs while maintaining clarity, rigor, and workforce relevance.

This paper is presented as a curriculum design case study and is therefore limited in scope to describing program structure, Knowledge Unit alignment, and assessment design. It does not provide longitudinal evaluation of student learning outcomes, employer satisfaction, or post-graduation placement, which are important indicators of workforce impact. Future work should evaluate the concentration using multiple evidence sources, such as analysis of student artifacts across cohorts, enrollment and retention trends, advisory or employer feedback, and alignment checks against evolving national SecureAI guidance. These evaluation steps would strengthen external validity and provide measurable evidence of how SecureAI curriculum design translates into workforce readiness.

11. Conclusions

The security of artificial intelligence is increasingly tied to national security outcomes, creating a clear need for educational pathways that address AI-specific threats and lifecycle risks alongside traditional cybersecurity foundations. Persistent workforce shortages, expanding AI adoption across high-stakes sectors, and a rapidly evolving adversarial landscape reinforce the importance of SecureAI programs that are grounded in formal Knowledge Units and supported by applied, practice-oriented assessment approaches (CyberSeek, 2025a; ISC2, 2024; National Centers of Academic Excellence in Cybersecurity, 2024; National Institute of Standards and Technology, 2023).

This paper presented the Illinois Tech SecureAI applied concentration as a case study in curriculum design. By embedding SecureAI into existing undergraduate and graduate

programs, and using a shared foundational cybersecurity technologies course delivered at two academic levels, the program structure supports efficiency while maintaining rigor through differentiated expectations and assessment depth. The four-course progression from cybersecurity foundations to AI foundations, SecureAI engineering, and AI risk governance provides a coherent pathway for building competencies aligned with national SecureAI guidance and workforce frameworks (MITRE, n.d.; National Centers of Academic Excellence in Cybersecurity, 2024; Petersen et al., 2020).

More broadly, the case study demonstrates how CAE-aligned institutions can extend established cybersecurity curricula to incorporate SecureAI without creating a separate degree program. As SecureAI frameworks and threat models continue to evolve, maintaining documented KU alignment and continuous curriculum review will remain essential to sustaining relevance and workforce impact. Future work can strengthen this curriculum-focused contribution through formal outcome evaluation, including longitudinal assessment of student artifacts, employer feedback, and post-graduation placement trends.

Author Contributions: Conceptualization, M.D. and S.Q.; methodology, M.D.; validation, M.D., A.B.A. and A.H.K.; formal analysis, M.D.; investigation, M.D. and S.Q.; resources, M.D. and A.B.A.; data curation, S.Q., A.B.A. and A.H.K.; writing—original draft preparation, S.Q.; writing—review and editing, M.D. and S.Q.; visualization, S.Q.; supervision, M.D.; project administration, M.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created.

Conflicts of Interest: The authors declare no conflicts of interest.

References

- Biggio, B., Nelson, B., & Laskov, P. (2012). Poisoning attacks against support vector machines. In *Proceedings of the 29th international conference on machine learning (ICML)* (pp. 1807–1814). Omnipress.
- Biggs, J., & Tang, C. (2011). *Teaching for quality learning at university* (4th ed.). Open University Press.
- Bishop, M. (2019). *Introduction to computer security* (2nd ed.). Addison-Wesley.
- Burley, D. L., Bishop, M., & Jones, E. (2018). Cybersecurity education: Bridging the gap between theory and practice. *IEEE Security & Privacy*, 16(5), 48–56.
- CAE Community. (n.d.). *About the NCAE-C program*. CAE Community.
- Carlini, N., Tramèr, F., Wallace, E., Jagielski, M., Herbert-Voss, A., Lee, K., Roberts, A., Brown, T., Song, D., Pierce, B. C., Thomas, K., Ippolito, D., Amodei, D., Radford, A., Sutskever, I., Clark, J., & Erlingsson, Ú. (2023). Extracting training data from large language models. In *Proceedings of the IEEE Symposium on Security and Privacy* (pp. 1–18). IEEE.
- Clear, T., Lister, R., Carter, P., Eckerdal, A., & Simon, B. (2018). Designing curricula for emerging computing disciplines. *Computer Science Education*, 28(3), 225–248.
- CyberAI Working Group. (2024). *Cyber AI programs “Stoneman” (version 1): Model and knowledge units for AICyber and SecureAI*. National Centers of Academic Excellence in Cybersecurity.
- CyberSeek. (2025a). *Cybersecurity supply and demand heat map*. Available online: <https://www.cyberseek.org/heatmap.html> (accessed on 31 December 2025).
- CyberSeek. (2025b). *CyberSeek expands cybersecurity workforce data coverage and enhances user experience*. Available online: https://www.cyberseek.org/docs/06-02-2025_CyberSeek_June_2025.pdf (accessed on 31 December 2025).
- Dawson, M. (2020). National cybersecurity education: Bridging defense to offense. *Land Forces Academy Review*, 25(1), 68–75. [CrossRef]
- Dawson, M. (2024). Integrating intelligence paradigms into cyber security curriculum for advanced threat mitigation. In *International conference on information technology—New generations* (pp. 77–81). Springer Nature Switzerland.
- Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. *Land Forces Academy Review*, 26(1), 69–75. [CrossRef]

- Dawson, M., & Omotoye, E. (2024, April). Combining cyber security and data science: A cutting-edge approach for public health education masters. In *International conference on information technology—New generations* (pp. 73–75). Springer Nature Switzerland.
- Dawson, M., & Szakonyi, A. (2020). Cybersecurity education to create awareness in artificial intelligence applications for developers and end users. *Scientific Bulletin*, 25(2), 50. [CrossRef]
- Dawson, M., Wang, P., & Williams, K. (2018). The role of CAE-CDE in cybersecurity education for workforce development. In *Information technology—New generations: 15th international conference on information technology* (pp. 127–132). Springer.
- Department of Defense. (2023). *DoD manual 8140.03: Cyberspace workforce qualification and management program*. U.S. Department of Defense.
- DoD Chief Information Officer. (2025, June 25). *Senior official promotes bolstering DoD cyber workforce*. U.S. Department of Defense. Available online: <https://dodcio.defense.gov/In-the-News/Article/4367443/senior-official-promotes-bolstering-dod-cyber-workforce/> (accessed on 31 December 2025).
- DoD Workforce Innovation Directorate. (n.d.). *DoD cyber workforce framework*. U.S. Department of Defense.
- Fredrikson, M., Jha, S., & Ristenpart, T. (2015). Model inversion attacks that exploit confidence information and basic countermeasures. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS)* (pp. 1322–1333). Association for Computing Machinery.
- Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015, May 7–9). *Explaining and harnessing adversarial examples*. Proceedings of the 3rd International Conference on Learning Representations (ICLR 2015), San Diego, CA, USA.
- Greshake, K., Abdelnabi, S., Scholten, R., Böttinger, K., & Fritz, M. (2023). Not what you’ve signed up for: Compromising real-world LLM-integrated applications with indirect prompt injection. In *Proceedings of the ACM Conference on Computer and Communications Security* (pp. 1–15). Association for Computing Machinery.
- ISC2. (2024). *(ISC)² publishes 2024 cybersecurity workforce study (first look)*. ISC2.
- Jagielski, M., Oprea, A., Biggio, B., Nita-Rotaru, C., Li, B., & Wang, B. (2018). Manipulating machine learning: Poisoning attacks and countermeasures for regression learning. In *2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, May 20–24* (pp. 19–35). IEEE.
- Kumar, R. S. S., Nyberg, E., & Wallach, H. (2023). Deployment risks of machine learning systems. *Communications of the ACM*, 66(8), 62–69.
- Lister, R., Adams, E. S., Fitzgerald, S., Fone, W., Hamer, J., Lindholm, M., McCartney, R., Moström, J. E., Sanders, K., Seppälä, O., Simon, B., & Thomas, L. (2016). A multi-national study of reading and tracing skills in novice programmers. *ACM SIGCSE Bulletin*, 36(4), 119–150. [CrossRef]
- Liu, Y., Neal, M., Jain, P., & Chen, D. (2024, May 7–11). *Trojaned retrieval-augmented generation models*. Proceedings of the 12th International Conference on Learning Representations (ICLR 2024), Vienna, Austria.
- Logan, P. Y., & Clarkson, A. (2015). Teaching cybersecurity through problem-based learning. *IEEE Security & Privacy*, 13(5), 53–56.
- MITRE. (n.d.). *MITRE ATLAS: Adversarial threat landscape for artificial-intelligence systems*. MITRE.
- Mulder, F., & Jansen, D. (2020). Building applied pathways in higher education for emerging technologies. *International Journal of Educational Technology in Higher Education*, 17(1), 1–15.
- National Centers of Academic Excellence in Cybersecurity. (2023). *CAE-CD designation requirements*. National Centers of Academic Excellence in Cybersecurity.
- National Centers of Academic Excellence in Cybersecurity. (2024). *PoS CyberAI program of study validation requirements*. National Centers of Academic Excellence in Cybersecurity.
- National Initiative for Cybersecurity Education. (2017). *Cybersecurity workforce framework (NICE Framework)*. National Institute of Standards and Technology.
- National Institute of Standards and Technology. (2023). *Artificial intelligence risk management frame-work (AI RMF 1.0) (NIST AI 100-1)*. U.S. Department of Commerce.
- National Institute of Standards and Technology (NIST). (2025, June 2). *New CyberSeek updates reveal 57,000 increase in cybersecurity job openings*. NIST.
- National Security Agency. (n.d.). *National centers of academic excellence in cybersecurity*. National Security Agency.
- Ngambeki, I. B., Rami, M., & Manson, D. (2021). Curricular improvement through course mapping: An application of the NICE framework. In *Proceedings of the ASEE annual conference & exposition, virtual conference, July 21–29*. American Society for Engineering Education.
- OWASP. (2025). *OWASP top 10 for large language model applications*. OWASP Foundation. Available online: <https://owasp.org/www-project-top-10-for-large-language-model-applications/> (accessed on 31 December 2025).
- Papernot, N., McDaniel, P., & Goodfellow, I. (2016). Transferability in machine learning: From phenomena to black-box attacks using adversarial samples. *arXiv*, arXiv:1605.07277. [CrossRef]
- Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z. B., & Swami, A. (2017). Practical black-box attacks against machine learning. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security* (pp. pp. 506–519). Association for Computing Machinery.

- Petersen, R., Santos, D., Smith, M., Wetzel, K., & Witte, G. (2020). *Workforce framework for cybersecurity (NICE Framework)* (NIST Special Publication 800-181 Rev. 1). National Institute of Standards and Technology.
- Scarfone, K., & Mell, P. (2012). *Guide to intrusion detection and prevention systems (IDPS)* (NIST Special Publication 800-94). National Institute of Standards and Technology.
- Shannon, C., & Weaver, W. (2019). *The mathematical theory of communication*. University of Illinois Press.
- Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017). Membership inference attacks against machine learning models. In *2017 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, May 22–26 (pp. 3–18). IEEE.
- Sweller, J., Ayres, P., & Kalyuga, S. (2011). *Cognitive load theory*. Springer.
- Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2014, April 14–16). *Intriguing properties of neural networks*. Proceedings of the 2nd International Conference on Learning Representations (ICLR 2014), Banff, AB, Canada.
- Tramèr, F., Zhang, F., Juels, A., Reiter, M. K., & Ristenpart, T. (2016, August 10–22). *Stealing machine learning models via prediction APIs*. 25th USENIX Security Symposium (pp. 601–618), Austin, TX, USA.
- Vassilev, A., Oprea, A., Fordyce, A., Anderson, H., Davies, X., & Hamin, M. (2025). *Adversarial machine learning: A taxonomy and terminology of attacks and mitigations* (NIST AI 100-2e2025). National Institute of Standards and Technology.
- Wang, P., Dawson, M., & Williams, K. L. (2019). Improving cyber defense education through national standard alignment: Case studies. In *National security: Breakthroughs in research and practice* (pp. 78–91). IGI Global.
- Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.
- Zhang, J., Chen, S., & Zhang, X. (2022). Secure deployment of machine learning models: A survey. *ACM Computing Surveys*, 55(6), 1–36.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.