ATARC

Cybersecurity Education and Workforce Development Working Group

powered by GovExec

JANUARY 2026

Chapter-Level Executive Summaries

The Convergence of AI-Cybersecurity in Education, Workforce Development, and Campus Infrastructure

Disclaimer:

This document was prepared by the members of the ATARC Cybersecurity Education and Workforce Development Working Group in their personal capacity. The opinions expressed do not reflect any specific individual nor any organization or agency they are affiliated with and shall not be used for advertisement or product endorsement purposes.

Terminology Note:

Throughout this document, the term "cybersecurity AI" is used interchangeably with "cyber-AI," "cybersecurity-AI," and "AI-cyber." These variations are intended for linguistic diversity and refer to the same set of technical frameworks and applications described herein

EXECUTIVE SUMMARY

This executive summary distills the core findings of the ATARC whitepaper examining the convergence of artificial intelligence and cybersecurity across education, workforce development, and campus infrastructure. The report concludes that AI and cybersecurity are no longer independent domains, but rather are converging into a unified operational, educational, and workforce reality with significant national security, economic, and societal implications.

Across K-12 and higher education, Cyber-AI literacy is now an essential skill for all learners, not solely technical specialists. Educational systems must evolve rapidly to integrate AI, cybersecurity, ethics, and digital citizenship across disciplines and grade levels. Higher education plays a critical role in aligning curricula, faculty development, and research practices with this converged reality.

From a workforce perspective, AI is redefining cybersecurity roles by accelerating automation while increasing demand for higher-order human judgment, governance, and ethical oversight. The report introduces a converged Cyber-AI workforce framework aligned to the NIST NICE Framework, emphasizing stackable credentials and lifelong learning.

For practitioners, AI functions simultaneously as a threat amplifier and a defensive necessity, requiring adaptive security architectures and continuous reskilling. Finally, the report highlights the urgent need for governance, policy, and oversight structures that keep pace with technological change while enabling innovation. Together, these findings underscore the need for coordinated national action to build a resilient, ethical, and future-ready Cyber-AI ecosystem.

01 ADVANCING CYBER-AI IN K-12 EDUCATION

Section Author: *Dr. Charles Gardner, EnterpriseKC*

This section establishes that AI and cybersecurity literacy must begin early and be sustained throughout the K-12 pipeline. Cyber-AI competencies are framed as foundational digital survival skills rather than niche technical abilities.

The chapter emphasizes developmentally appropriate, scaffolded instruction that progresses from basic digital citizenship and AI awareness in elementary grades to applied cybersecurity scenarios, machine learning concepts, and ethical analysis in high school.

Cross-disciplinary integration is central, embedding AI and cybersecurity across mathematics, science, social studies, arts, and career and technical education. Real-world, community-based projects anchor learning in practical outcomes. Ethics, privacy, and student data protection are treated as core requirements. The chapter concludes by emphasizing teacher upskilling and collaboration among families, schools, industry, and higher education.

02 ADVANCING CYBER-AI IN HIGHER EDUCATION

Section Author: *Dr. Keith Clement, California State University, Fresno*

This section positions higher education as the structural backbone of the Cyber-AI ecosystem. Colleges and universities must adapt curricula, pedagogy, and research practices to an AI-driven environment. The chapter highlights the diversity of U.S. higher education and the challenge of delivering consistent Cyber-AI education at scale.

Converged curricula spanning cybersecurity, AI, data science, law, and ethics are emphasized. Faculty impacts and institutional risk considerations are addressed directly. Cyber-AI literacy is framed as a universal graduate competency. The section concludes with recommendations for curriculum modernization, faculty development, and strengthened industry and government partnerships.

03 ADVANCING CYBER-AI WORKFORCE DEVELOPMENT

Section Author: *Dr. Keith Clement, California State University, Fresno*

Section 3 introduces a new, converged Cyber-AI Workforce Development Architecture Framework aligned to the NIST NICE Framework. The framework is designed to reflect how artificial intelligence is fundamentally reshaping cybersecurity work roles, required skills, and career pathways across the entire professional lifecycle.

Rather than treating AI as a supplemental technical skill, the framework integrates AI capabilities directly into cybersecurity role definitions, training pathways, and competency models at the entry-level, intermediate, advanced, and executive tiers. This approach supports both traditional academic pathways and non-traditional, skills-based routes into the profession, including certifications, apprenticeships, and continuous professional education.

The chapter emphasizes workforce evolution rather than workforce displacement. Human-in-the-loop models remain essential for governance, strategic decision-making, ethics, and accountability. The framework is intended to guide educators, employers, and policymakers in aligning curriculum design, credentialing strategies, and workforce investment to support scalable, future-ready Cyber-AI talent pipelines.

Phase 1: Foundations (Weeks 1-4)

Module	Skills Developed	Framework Alignment
Cybersecurity Essentials	CIA triad, threat types, IAM encryption	NICE: PR-CDA-001
Python for Security-AI	Scripting, automation, data parsing	NICE: OM-DE-001
Networking & Cloud Basics	TCP/IP, DNS, Cloud platforms, IAM	NICE: IN-NET-001

Phase 2: AI Literacy for Security (Weeks 5-8)

Module	Skills Developed	Framework Alignment
Intro to Machine Learning	Learning models, evaluation	NIST AI RMF: Map, Measure
Adversarial ML & Model Risks	Evasion, poisoning, inversion	NICE: SP-RSK-002
AI Ethics & Governance	Bias, fairness, ISO/IEC 42001	NICE: OV-GOV-001

Phase 3: Applied Security (Weeks 9-12)

Module	Skills Developed	Framework Alignment
SIEMs & Threat Detection	ELK, anomaly detection	NICE: PR-INF-001
Secure AI Deployment	Model monitoring, API security	NIST AI RMF: Manage
Hands-on Labs & CTFs	Red/blue team, adversarial ML	NICE: PR-CDA-001

04 FROM STATIC DEFENSES TO SELF-EVOLVING SYSTEMS: THE SECURITY PRACTITIONER'S AI IMPERATIVE

Section Authors: *Eric Wall, CISSP, CISM, University of Arkansas System; Gregory W. Cooper, New Mexico State University*

This section provides a practitioner-focused view of AI's impact on cybersecurity operations. AI is both a threat amplifier and a defensive necessity. Threat actors increasingly leverage AI for scale and sophistication, while defenders rely on AI for detection, response, and automation.

Ethics, privacy, and bias are treated as operational risks. Securing AI systems introduces new threat vectors requiring specialized controls. The chapter concludes by emphasizing adaptive architectures, continuous reskilling, and governance structures that preserve human accountability in AI-augmented security environments.

05 CYBER-AI LEGISLATION, GOVERNANCE, AND OVERSIGHT

Section Author: *Emily Harris, J.D., CISSP, CIPP/US, Higher Education Cybersecurity Professional*

This section examines the evolving legal and regulatory landscape governing AI and cybersecurity. It contrasts U.S. and EU approaches and highlights the lag between technological change and policy development. The chapter explains how legislation and organizational policy influence education, workforce development, and institutional risk management.

Organizational governance is positioned as the most immediate control mechanism. The section concludes with recommendations for coordinated policy action and alignment across governance, education, and workforce systems.