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

Advanced Technology Research Center (ATARC)

ATARC Cybersecurity Education and Workforce
Development Working Group

January 2026

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

Report Authors

Dr. Keith Clement, California State University, Fresno, ATARC Cybersecurity Education & Workforce Development Academic Chair

Eric Wall, CISSP, CISM, University of Arkansas System, ATARC Cybersecurity Education & Workforce Development Academic Co-Vice Chair

Gregory W. Cooper, Head of ISOC, New Mexico State University, ATARC Cybersecurity Education & Workforce Development Academic Co-Vice Chair

Dr. Charles Gardner, EnterpriseKC

Emily Harris, J.D., CISSP, CIPP/US, Montclair State University

Strategic Action Plan and Recommendations Report prepared for the 119th U.S. Congress and National Association of State Chief Information Officers (NASCIO)

**Advanced Technology Research Center (ATARC)**

**ATARC Cybersecurity Education and Workforce Development Working Group**

**January 2026**

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.

# Executive Summary

The science fiction future of the 20th Century has arrived. Wristwatch communication devices, internet-linked sunglasses, self-driving cars, home drone delivery services, flying jetpacks and cars. What an amazing time of rapid global technology innovation and transformation with new devices, apps, social media, and all. AI has deeply captured the global community imagination since generational AI and ChatGPT erupted into the market a few short years ago. Agentic AI and automation are further moving the needle of change and strategic calculations to build and sustain AI driven comparative advantage (economic and security) across the world. Many consider this new tech age as the dawning of the AI era.

The importance of securing the digital world (cybersecurity) has been understood for decades. However, the cybersecurity eco-system has been deeply impacted by the rise of AI, Machine Learning, and Quantum Computing in numerous direct and indirect ways. Malware, ransomware, supply chain attacks, stolen credentials, data breaches, and other attacks continue to make the daily news. International cybercrime accounted for $10.5 trillion dollars in losses in 2024 and is expected to grow over the next decade. AI is expected to be utilized to facilitate a growing role in increasingly sophisticated cyberattacks and cybercrimes. Cybersecurity and AI are critical capabilities moving deeper into the digital age.

Like two mighty rivers, we are now watching a “convergence” of streams between AI and Cybersecurity. By convergence we mean that AI and Cybersecurity are increasingly related and impactful of one another in numerous ways. Convergence comes with many profound national implications—economic, political, social, and cultural. AI is significantly altering cybersecurity operation, best practices, and the “playbook.” At the same time, there is a growing need and concern of securing AI systems, models, and tools through proactive digital and physical security strategies. We must rewrite the incident response playbook given the evolving impact of AI on all things cybersecurity to reduce, manage, mitigate, and respond.

Emerging technologies like AI and cybersecurity may have a potential disruptive effect as we figure out the new risks, vulnerabilities, and impacts upon the Cyber-AI era. The U.S. must prepare for these tech challenges today. Securing AI and Cyber is a rapidly growing and significant national and economic security problem. Nowhere is this convergence playing out more than in our school districts, colleges, universities, workforce, and campus infrastructure nationwide. Why? Because we are talking about the profound impact that Cyber-AI is having on school, districts, colleges, and universities, including faculty teaching, student learning, research capacity, and workforce development.

# Executive Summary

In this white paper we describe and analyze advancing AI transformation in K-12 and Higher Education. Understanding these new realities is critical in designing the necessary learning architecture and curriculum driving future efficient preparation processes for the next generation of Cyber-AI professionals. What skills, knowledge, and tools do future Cyber-AI professionals need to have to be successful in the field? This paper will recommend the development of a new work-role to support the preparation of Cyber-AI professionals at all levels of the career ladder (entry-level, intermediate, advanced, and executive level work roles) and provides an aligned and linked stackable curriculum as a baseline starting point. This Cyber-AI work role is discussed in greater detail in report section 3.

Furthermore, given the critical and fundamental nature of converged AI and Cyber skills and capabilities today across society, we must elevate these skill sets across all learners and workers in the U.S. Cyber-AI skillsets are so important in a digital world. We must teach U.S. students these skills and competencies early and throughout the professional and education preparation processes. Cyber-AI skills are now Soft Skills (or, “Essential Skills”) given their growing importance in the digital world around us. Cyber-AI skills are growing in value for the employers of today. We must not only must prepare the next generation of Cyber-AI specialists to work in this domain, but everyone advancing into the future workforce. This new skillset is increasing in value across all occupations and sectors in the economy.

The U.S. has long been working to tackle a cybersecurity capability and skill gap. Today, AI is further complicating this incredibly important policy area. One purpose of this report is to analyze the impact of the convergence of Cyber-AI from a variety of key perspectives. This report analyzes, evaluates, and provides policy recommendations from a community of Higher Education and Workforce Development Subject Matter Experts (SMEs) in cybersecurity, AI, and campus tech infrastructure. SMEs reflect many perspectives and are drawn from key stakeholders including industry, government, academe, and Non-Government Organizations (NGOs). As this is an increasingly and incredibly complex policy area (i.e. the nexus of where AI and cybersecurity are converging), analysis, evaluation and report recommendations are found in the following subject areas. These subjects are discussed at length further in this report and the recommendations contained here within.

**Key report findings and recommendations are found in the following report sections:**

- Advancing Cyber-AI in K-12 Education (Section 1)
- Advancing Cyber-AI in Higher Education (Section 2)
- AI-Cybersecurity Workforce Development (Section 3)
- Campus Practitioners and Infrastructure (Section 4)
- Legislation, Governance, and Oversight (Section 5)

**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.

# Table of Contents

# Table of Contents

# Table of Contents

# Table of Contents

# Table of Contents

# Acknowledgements

This white paper, writing project, and AI-Cybersecurity workforce development and education recommendations are the collaborative work of many contributing Subject Matter Experts (SMEs). We acknowledge everyone for their work, diligence, and efforts completing this report. Our sincere apologies for those who may have contributed to the research and paper, but were left off the acknowledgements list inadvertently.

Kevin Sanchez-Cherry, Cybersecurity Policy, Training, and Workforce Lead, U.S. Department of Transportation

Cindy Ramboyong, Science & Technology Engagement and Analysis Division, Virginia Tech Applied Research Corporation

Joe Boye, Solutions Consultant Manager, Palo Alto Networks Public Sector, LLC

Willie Henderson, Business Development Manager, Cyber Innovation Center

# Commonly Used Abbreviations

Accepted Use Policies (AUP)
Advanced Placement courses (AP)
Advanced Technology Academic Research Center (ATARC)
Artificial Intelligence (AI)
Augmented Reality (AR)
Application Programming Interface (API)
Association for the Advancement of Artificial Intelligence (AAAI)
Blind and Visually Impaired (BVI)
Broward County Public Schools (BCPS)
Business Email Compromise (BEC)
California State University (CSU)
Capture the Flag (CTF)
Career Technical and Community Education (CTACE)
Career Technical Education (CTE)
Center of Academic Excellence (CAE)
Chief Digital and Artificial Intelligence Office (CDAO)
Chief Information Security Officer (CISO)
Cloud Security Posture Management (CSPM)
Computer Fraud and Abuse Act (CFAA)
Common Vulnerabilities and Exposures (CVE)
Common Online Data Analysis Platform (CODAP)
Community Based Organizations (CBOs)
Computer Science Teachers Association (CSTA)
Consortium for School Networking (CoSN)
Critical Infrastructure Protection (CIP)
Department of Defense (DoD)
Department of Homeland Security (DHS)
Enterprise Kansas City (EKC)
European Union (EU)
Extended Detection and Response (XDR)
Federal Bureau of Investigation (FBI)
Federal Education Records and Privacy Act (FERPA)
Health Insurance Portability and Accountability Act (HIPAA)
Human in the Loop (HIL)
Human Resources (HR)
General Data Protection Regulation (GDPR)
Graphical User Interface (GUI)
Incident Response (IR)
Indicators of Compromise (IOCs)
Information Technology (IT)
Inquiry-Based Learning (IBL)
Internet of Things (IoT)
Intellectual Property (IP)
Identity Access Management (IAM)

# Commonly Used Abbreviations

Know Your Customer (KYC)
Large Language Models (LLMs)
Machine Learning (ML)
Massachusetts Institute of Technology- Responsible AI for Social Empowerment and Education (MIT RAISE)
National Association of Higher Education Systems (NASH)
National Centers of Academic Excellence in Cybersecurity (NCAE-C)
National Center for Education Statistics (NCES)
National Initiative for Cybersecurity Education (NICE)
National Institute of Standards and Technology (NIST)
National Oceanic and Atmospheric Administration (NOAA)
National Science Foundation (NSF)
National Security Agency (NSA)
Natural Language Processing (NLP)
National Student Clearinghouse Research Center (NSCRC)
Non-Government Organizations
Not for Profits (NFPs)
On the Job Training (OJT)
Organisation for Economic Co-operation and Development (OECD)
Personally Identifiable Information (PII)
Problem-Based Learning (PBR)
Professional Development (PD)
Protected Health Information (PHI)
Responsible AI for Computational Action (RAICA)
Science Technology Engineering and Mathematics (STEM)
Science Technology Engineering Arts and Mathematics (STEAM)
Security Information and Event Management (SIEM)
Security Operations Center (SOC)
Security Orchestration, Automation, and Response (SOAR)
Self-Regulated Learning (SRL)
STEM Learning and Research Center (STELAR)
Subject Matter Expert (SME)
Tactics, Techniques, & Procedures (TTPs)
Trusted Execution Environments (TEE)
University of Florida, AI for K-12 Initiative (AI4K12)
University of Florida's Engaged Quality Instruction through Professional Development Program (EQuIPD)
United Nations Educational, Scientific, and Cultural Organization (UNESCO)
United States Code (U.S.C.)
User Behavior Analytics (UBA)
World Economic Forum (WEF)
World Wide Web (WWW)
Zero Trust Architecture (ZTA)

# About Advanced Technology Academic Research Center (ATARC)

### The Advanced Technology Academic Research Center (ATARC) is where government missions meet innovation and collaboration.

**ATARC is not a think tank**—it is a technology integration hub that unites leaders from government, industry, and academia to tackle complex innovation challenges. Instead of producing abstract recommendations or theoretical models, ATARC focuses on applied collaboration, helping the Federal government understand, evaluate and integrate emerging technologies in operational contexts.

Through interactive events, hands-on Working Groups and focused technical exchanges, ATARC enables government stakeholders to engage directly with innovators. These engagements provide meaningful, low-barrier opportunities for agencies to explore market-ready solutions, gather insights from field-tested practices, and inform procurement and policy decisions with real-world experience—not detached analysis.

ATARC's mission is to foster results-oriented public-private collaboration that drives modernization and advances mission effectiveness. Whether through curated technology showcases, mission-focused roundtables, or strategic technical exchanges, ATARC serves as a trusted advisor and catalyst for impactful change.

We don't just talk about innovation—we help agencies deploy it. Join us in shaping the future of government technology through purpose-driven collaboration. [1]

### ATARC Cybersecurity Education and Workforce Development Working Group Mission Statement

"Build a collaborative framework of key stakeholders to provide strategic recommendations on enhancing national cybersecurity education and workforce development policy and practice to implement an innovative and  comprehensive national career pipeline/ pathway at all levels of education/training, accessible to everyone, and clearly communicated through detailed "road maps" for career preparedness and college readiness tracks." [2]

[1] **https://atarc.org/about/** Accessed electronically on 9/3/2025.

[2] **https://atarc.org/cyber-higher-education/** Accessed electronically on 8/30/2025.

# About Advanced Technology Academic Research Center (ATARC)

### ATARC Cybersecurity Education and Workforce Development Working Group Objectives

1. Develop and maintain working group collaboration and partnerships to complete a number of activities, initiatives, deliverables, and pilot projects in progress. It is critical that industry (employers), academia, the public sector, and community/ neighborhood-based organizations work together collaborating and craft viable solutions.

2. Enhance and support national and state-level cybersecurity education, workforce development, and initiatives through pilot program design, implementation, and evaluation.

3. Understand, analyze, and evaluate cyber policies, best practices, and common ways of professional preparation into quickly evolving "hard-to-fill" positions currently within the cybersecurity field.

4. Align, link, and coordinate cybersecurity education, training, and workforce development practices into a seamless, easy to transition career education pipeline and pathway spanning K-12 Education and Higher Education and transition into the workplace that includes both a "traditional approach" (academic) and "non-traditional approach" (skills based).

5. Work with academics and practitioners to understand the core obstacles, limitations, and challenges facing key stakeholders and major partners in AI-Cybersecurity workforce development and education.

# Introduction and Context

### Artificial Intelligence and Machine Learning

Artificial Intelligence (AI) and Machine Learning (ML) are changing the world daily. AI gains in intelligence every single day. AI evolves at an amazing pace and will continue into the foreseeable future. Its evolution is difficult to predict in this early day of the AI epoch. AI is growing in impact in our organizational and individual lives. Emerging technology is deeper embedded into our societies and culture. Humans utilize AI daily and in more profound ways. We are taking steps from the physical world into the virtual and digital world and piloted by AI systems, models, algorithms, and tools.

Remarkable tech transformation and machines are changing many aspects of human activity, impacting security, workforce, education, training, and campus critical digital infrastructure. Far reaching changes are occurring in many policy areas as a direct result AI's growing influence worldwide. AI is highly impactful on the global economy, security, and culture. Rapid and significant changes are raising legitimate questions and potential areas of concerns with issues like risk management, expectations of privacy, sound governance, policy, regulation, oversight, and compliance. New forms of AI systems, models, and tools evolve quicker than laws, policy, and potential regulation. AI evolution is changing cybersecurity and information practices, operations, best practices, and frankly the entire playbook.

Generative AI, Agentic AI, and Automated AI can enhance offensive and defensive cybersecurity operations in a variety of ways. There is more AI automation today in both blue and red team operations and activities. Quality big data analysis and tools will be critical in the coming years as societies rely on AI to summarize, analyze, and make consequential decisions in our lives. We will continue to see a reduction in human activity sifting through and analyzing large data sets. As such, policy-makers, industry, academe, and Non-Government Organizations (NGOs) struggle with the implementation and utilization of effective and ethical AI systems and how machines and humans are to interact effectively from here and into the future.

The AI era promises great things and is beginning to deliver. Machine learning and "deep learning" is impacting human security, cognition, and learning. Deploying and securing AI raises profound risks that are not completely understood. These risks must be better understood to develop proactive strategies and approaches moving forward. Cyber-AI issues are growing in importance as we discuss technological convergence and its remarkable potential future implications.

This report seeks to provide guidance and direction to federal and state decision and policy-makers in making critical adjustments to advance Cyber-AI education and workforce development soon. In a world characterized by tech and data, the value of skilled cybersecurity professionals is bound to increase. Preparing the American citizenry, worker, and student for success with Cyber-AI skills in the 21ST Century begins early in the educational process and continues throughout the workforce and all rungs of the career ladder.

# Introduction and Context

## Cybersecurity

Cybersecurity issues confront all nations and serves to challenge international economics, politics, societies, organizations and individuals. In a tense geopolitical world, cyberattacks, information warfare, and state-level espionage are changing the rules of both peace and conflict. AI is impactful here as new technologies increase uncertainty, promulgate change, new security risks, and opens up new potential vulnerabilities to be effectively manage. Due to the fundamental need for cybersecurity in the current geopolitical situation, a natural area of substantial AI evolution has been within the domain of cyber- and physical security.

The impact of AI on a fraught cybersecurity environment (which is discussed shortly) has deep and fundamental implications for the direction of these technologies and what is defined as "reasonable and ethical use" of AI and Cybersecurity. Broad impacts on government, industry, and academe in the cybersecurity domain are sending tremendous shockwaves into how we govern, business operates, and educational institutions teach. The speedy pace of technology has accelerated quickly with grand innovations in AI, deep learning, high-speed quantum computing, and securing tech is an exponentially growing challenge. We must be prepared for the future digital workforce and the critical cybersecurity domains found within the NICE Framework:

With over ten trillion dollars in losses last year globally, billions of user data breached, cybersecurity problems are nothing new. Cybersecurity issues are compounded by a critical need to secure AI systems, models, and tools now too. The relationship between AI and cyber is growing closer with many intertwined implications. For example, true given the current number of devices in the Internet of Things (IoT). The number of IoT devices worldwide is forecast to more than double from 19.8 billion in 2025 to more than 40.6 billion IoT devices by 2034.  IoT devices are found in critical infrastructure sectors. IoT devices are found in the consumer internet and media devices (like smartphones).  They are found in many common items that must be secured like cars, TVs, electronics, and appliances. What is key to note is that IoT devices are a prime example of the processes of convergence underway between AI and Cyber technologies, processes, innovations, and growing interactions.

The purpose of this report is to analyze and discuss these implications in Cyber-AI education, workforce development, campus infrastructure, governance, and oversight. This subject is salient to decision-makers due to significant strategic implications for a prepared Cyber-AI Workforce, secure campus infrastructure, and the law and policy of emerging technologies in a growing and changing AI world. In the next few pages, we will be defining and discussing key concepts and terms.

[3] **https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/** Accessed electronically on 9/22/2025.

[4] **https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/** Accessed electronically on 9/22/2025.

# Introduction and Context

### The Convergence of AI and Cybersecurity

There are numerous implications and ramifications following tremendous global tech leaps and widespread utilization. Just like major highways and mighty rivers come together and change the course of both, the process of technological convergence in AI and cybersecurity is ongoing and bound to fundamentally impact both. Rapid technological innovation poses significant strategic questions and operational challenges for key actors and major stakeholders worldwide. AI and cyber are converging in ways that are not yet commonly understood and will have substantial impacts on the future of the international world order and the U.S.

In a world characterized by tech and data, the value of cybersecurity and AI professionals is bound to increase. It is safe to say that AI is rapidly changing cybersecurity and the education/ learning preparation process, digital campus technology infrastructure /services, and the actual workplace. The convergence of Cyber-AI is happening in multiple ways:

1. **Given the critical nature of Cyber-AI skills in a digital age—these should now be considered "Soft Skills" or "Essential Skills" for everyone that uses computers, browses the internet, utilizes e-mail/social media, and/or has a smart device (like a cellular phone/tablet, etc.).** In this way, Cyber-AI skills are required for all who participate in educational attainment, in the workforce, or operate in the contemporary digital environment, social media, checking e-mails, downloading apps, etc. Cyber-AI literacy, awareness, and preparedness must be taught to everyone, starting young (i.e. preK-12), and for all ages of the population. Research indicates that the young, old, and non-tech savvy are particularly vulnerable to cybercrimes and related issues like privacy, online scams, etc.

2. **"Converged "Cyber-AI" work roles will look vastly different at all levels of the career ladder from entry level to executive-level positions within all sectors of the economic and occupational clusters.** In other words, AI is changing the nature of work roles and job descriptions themselves (both literally and figuratively). As the duties, tasks, and responsibilities of cybersecurity professionals change on the job, then the job preparation process must be revisited and revised by what is becoming the new reality of the AI era. The future shape of workforce is a critical implication with the technological convergence of Cyber-AI.

**This report includes a detailed architecture and structure for an Cyber-AI Converged Work Role stacking curriculum framework and map aligned and linked for all levels of the career ladder: entry-level, intermediate, advanced and executive level work roles.** The framework is aligned with the NIST NICE Framework, and professional industry-based certifications for a career pipeline/pathway, onboarding programs, and strategic workforce development.

# Introduction and Context

### Further Cyber-AI Convergence in Education and Workforce Development

We are watching a massive restructuring in how we learn, what we learn, and these new trends and morphing the workplace and how we prepare skilled professionals. Schools, Colleges, and Universities are undergoing transformative change as AI impacts the classroom, faculty, administration and students. We have much to learn, as learners, workers, and global citizenry in effective AI utilization, literacy, responsible and ethical use, and general Cyber-AI preparedness and awareness skills. AI-Cybersecurity Education (K-12 and Higher Education), workforce development, campus IT infrastructure, government law, policy, and oversight. Emerging technology innovations advance much faster than the development and implementation of academic programs, so maintaining “up-to-date” curriculum programs, and workforce development opportunities must change quickly to keep pace.

We should not underestimate the value of strategic thinking in the utilization of AI to enhance national economic and security. AI has remarkably transformed the pace of this innovation and ensuing education and workforce development capability and skills gap. We must ensure to properly prepare the current and future generation of security professionals moving into the AI era. It is time to have a discussion of the trend of convergence between AI and cybersecurity. AI is fundamentally reshaping and transforming security architecture from top to bottom of the tech ecosystem. Both blue team (defense) and red team (offensive) security plans, activities, processes, and work roles are being significantly impacted.

It is important to maintain and strengthen comparative advantage with American strategic adversaries in AI. The only way forward is to enhance Cyber-AI Education and Workforce Development capacities and capabilities in a variety of important dimensions such as education and training; curriculum and content; instructional strategies (teaching/pedagogy); linkages with professional industry-based certifications; workforce opportunities (like paid internships and registered apprenticeship programs); and professional development/socialization opportunities available to everyone. Campuses and educational institution must be secure and safe environments to learn and become more cybersecure. Furthermore, we must make similar transformative changes to how we educate and prepare this and the next generation of skilled AI and cybersecurity professionals. These are key issues discussed throughout the report.

# Introduction and Context

### Statement of the Problem

Before getting into details, we discuss several key core problems underpinning our report on Cyber-AI Convergence and related issues impacting school, college, and university campuses. Societal cybersecurity concerns have been ongoing and making headlines for years. Reports of cyber threats, attacks, data breaches, identity theft are commonplace. Many organizations and individuals are rightfully concerned about their digital security and online privacy. In 2025, AI (generative, agentic, automation) is dramatically impacting an already fraught cybersecurity domain. AI is rewriting the cyber game plan for blue team (defenders) and red team (attackers/ethical hackers) in terms of threat hunting, threat intelligence, incident response, strategic planning, and numerous other ways. Significant changes have also been experienced for the K-12 and Higher Education communities, training organizers, and workforce development specialists. Evolving AI capabilities, strategies, and tools can assist both blue teams and red teams (and how they interact amongst themselves).

Just like with security and prevention, sometimes the red team attackers have the upper hand due to their advanced use of technology and gaps within existing frameworks, laws, policies, and regulations. These high impact issues of securing AI and our digital environment will ultimately become the purview of legislators and decision makers as we seek political and legal solutions to the scourge of cybercrime, Critical Infrastructure Protection (CIP), international/national malicious threat actors, state sponsored espionage, Intellectual Property (IP) losses, and general industrial/consumer fraud and theft.

Implications play out as we discover intended (transformative) and unintended (disruptive) consequences of AI in a whole host of broader policy areas, as well as specifically within cybersecurity and Information Technology (IT). Automation offers organizations potential substantial benefits, competitive advantages, reduced personnel and overhead costs (i.e. laying off the human security team members), and additional productivity gains given efficient autonomous AI utilization and tools. AI comes with economic costs, vast use of power and water resources, as well as human and financial costs related to potential economic displacement and impact of deepening societal change. How is AI impacting the labor market and the rates by which jobs are taken or made? It is currently unclear.

It is of vital national interest that we chart an innovative and thoughtful strategic approach to AI with an eye towards a significant capability and capacity building and enhanced American cybersecurity and cyber-defense posture. This issue is exacerbated as all sectors of the economy (public and private) struggles with the implementation and utilization of Cyber-AI and these new skills and critical competencies leading to a skilled national workforce. To do so, we will analyze the problems of Cyber-AI convergence as related to all aspects of education, workforce development, and campus infrastructure, evaluate this topic in terms of solution building, and then provide a series of recommendations moving forward here.

# Introduction and Context

### Key Concepts and Terms Defined

Prior to discussing the specifics within each report section (5), we define important subject concepts and terms found extensively in this report. After we analyze these key definitions, we will discuss a conceptualization of AI and Cybersecurity convergence and its implications in U.S. education, workforce development, campus infrastructure protection and provide recommendations relating to governance and oversight in this growing policy area. Definitions are provided for key terms/concepts including AI, Cybersecurity, Machine Learning, and Convergence.

**Artificial Intelligence Defined:**

1. **From 15 U.S.C. 9401(3): Official definition of AI used in all federal legislation, and minor variations are used in state legislation:** The term "artificial intelligence" means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to— (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action.

2. **Organisation for Economic Co-operation and Development (OECD) AI definition:** *An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.*

3. **AI Defined:** "the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience." [5]

   Generative AI-

   Agentic AI-

   AI-Automation-

**Machine Learning Defined:**

"Machine learning (ML) is a type of artificial intelligence that **allows machines to learn from data** without being explicitly programmed. It does this by optimizing model parameters (i.e.

[5] https://www.britannica.com/technology/artificial-intelligence Accessed electronically on 9/4/2025.

internal variables) through calculations, such that the model's behavior reflects the data or experience. The learning algorithm then continuously updates the parameter values as learning progresses, enabling the ML model to learn and make predictions or decisions based on data science. The applications of machine learning are wide-ranging... Overall, machine learning plays a crucial role in enabling computers to learn from experience and data to improve performance on specific tasks without being programmed. It has the potential to revolutionize various industries by automating complex processes and **making intelligent predictions or decisions** by "digesting" vast amounts of information."

**Cybersecurity Defined:** "Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information." [6]

**Convergence Defined: Convergence: noun.**

"The process or state of converging; the property of converging." [7]
"In technology, convergence involves the integration of different technologies into a single device or system." [8]

AI and Cybersecurity are moving closer together with significant ramifications and impacts on each sector individually. However, this convergence is also evolving into a new form and structure and creating something new here- an AI-Cybersecurity Convergence that is the focus of this research white paper.

GRAPHIC #1:

There are many important relationships found (and continuing to grow) as AI and cybersecurity become more closely integrated through the processes of converging technologies.

1. Cybersecurity is heavily impacted by AI on both Blue Team (defenses) and Red Team (attackers/ethical hackers).

2. AI Systems, Models, Algorithms, and Data must be secured.

3. Cybersecurity and AI are both evolving, maturing, and interacting in this convergence of two extraordinarily emerging technologies.

Because of these critical implications of the relationship between Cyber-AI, we discuss convergence as upcoming outcome to gain understanding as the future continues to arrive.

[6] https://www.cisa.gov/news-events/news/what-cybersecurity Accessed electronically on 9/4/2025.
[7] https://finesentence.com/meaning/convergence Accessed electronically on 9/4/2025.
[8] https://finesentence.com/meaning/convergence Accessed electronically on 9/4/2025.

# Introduction and Context

### The Convergence of AI and Cybersecurity: Workforce Development and Education

Key terms and concepts were defined contextually in previous report section. It is critical to discuss the term "convergence" and how it is impacting societally broadly. We also seek to illustrate the connection, describe the relationship, and point out implications as AI and Cyber continues the path to convergence. There are numerous significant implications found at the nexus of AI and Cybersecurity. For purposes of this report, we limit this inquiry of Cyber-AI convergence and impact on K-12 Education, Higher Education, Workforce Development Campus Infrastructure and Technology Practitioners, and governance, policy, law and oversight.

Convergence in going on broadly across the global and tech environment and impacting the U.S. significantly. Convergence is the process by which different entities, ideas, or systems come together and become more integrated. It can refer to a wide range of phenomenon including technological, social, and mathematical concepts. [9] There are many important relationships found (and continuing to grow) as cybersecurity and AI become more closely integrated as 2025 progresses:

GRAPHIC #2:

1. Cybersecurity is heavily impacted by AI.
2. AI and data have significant need to be secured.
3. AI has been a game changer for both red and blue cyber teams.
4. Sophisticated AI-infused threats, exploits, attacks, breaches, etc., as well as the power of automating attacks and defenses.
5. The high value of securing AI and data through physical and digital security.

    - Understand the foundational basics (from computer science- data, hardware, software, etc. ). The impact of the internet launch in the early 1990s. AI is going to be as transformative technology has proliferated and grown to other many other academic disciplines and professional fields. As such, we have a massive amount of catch-up.
    - AI-Cybersecurity-IT Convergence- this proliferation is going on full steam- we need to make sure everything is covered in this nexus. Lot of challenges and opportunities-

[9] Lumen Learning, Media, and Culture, link

# Introduction and Context

- Understand the link between AI-Cybersecurity (Broadly Speaking)
- Understand the link between AI-Cybersecurity & WDE
- How to support Cyber-AI Education and Workforce Development
  - How to inspire teachers and students-
  - How to support educational institutions (Schools, Colleges, Universities)
  - How to support a non-academic pathway into AI-Cybersecurity-
  - Ensure significant resources and guidance are available within the ecosystem-

**Key Report Question:** What is the challenge of Cyber-AI Convergence in education, workforce, campus infrastructure, governance and policy?

**Answer:** The breadth and depth of AI-Cybersecurity career and occupational clusters must evolve with this new reality in mind as we contemplate what the future of this workforce will look like and the preparation process to get them into the professional world and the career ladder; while simultaneously protecting campus digital and technology services.

**Justification:** AI and Cybersecurity cross all sectors of society, the economy (public, private, Not for Profits (NFPs) and Community Based Organizations CBOs) as well as all industry sectors, including Critical Infrastructure Protection (CIP). The convergence of AI and cybersecurity is heavily transforming our society and technology. The following section of the report discusses the paper organization and structure utilized in this white paper.

**White Paper Project Purpose:** To prepare a white paper analyzing and evaluating the converging role of AI in Cybersecurity in the domains of K-12 Education, Higher Education, and Workforce Development. There are numerous perspectives to include in this research and recommendations-based report. Subject Matter Experts (SMEs) and drawn from many key sectors including the government, industry, and academia.

1. What are the implications for AI in the cybersecurity domain?

   A. Impacts on both Red Team & Blue Team game plan, operations, and activities.

# Introduction and Context

B. Many cybersecurity domains, tasks, KSAs and work-roles are significantly impacted by Generative AI/Agentic AI. AI Automation will replace an unknown number of cybersecurity professional jobs (i.e. automation), but not all of them. These skills and competencies of converged Cyber-AI positions (entry, intermediate, advanced, and executive-level) that are laid out in report section 3. There are still physical security concerns, management positions, and Human in Loop (HIL) personnel needed—even in generally autonomous AI-cybersecurity stacks and machine centric architectures.

C. Understanding the current and future broader implications of AI in Cyber. What is the future of cybersecurity in the AI era? For example, perhaps a future digital environment characterized by automated AI attacks against AI-infused defenses. Pressure is mounting on organizations (government and enterprise) to include more AI into their defensive architecture to reduce incident response time (and financial costs!). If AI and machines continue to rise securing the digital environment, that would suggest in a zero sum game of impacting human cybersecurity professionals and employment opportunities. This issue may be of additional concern further in the report in AI policy and legislation to enhance the role of law and policy to maintain the importance of humanity in security, guardrails, compliance, and oversight (please see Section 5).

D. What are the future implications of AI from a legislative, regulatory, legal, and oversight issues in the U.S. and European Union (E.U.). Many of these implications and costs are just now coming to light. For example, not yet evident.

2. Understand the implications of a convergence of AI & security in Workforce Development and Education to best protect society, organizations, and individuals.

3. We must better understand this connection prior (i.e. AI and risks, threats, and vulnerabilities) before getting into governance and policy issues that are addressed by meaningful program and course curriculum, content, teaching pedagogy, labs, exercises, etc.

4. In addition, additional education experiences workforce/experiential opportunities like pre-apprenticeship programs, registered apprenticeship programs, internships, and industry based professional certifications.

5. How do we build an Cyber-AI workforce development and education (WDE) framework (including K-12 and Higher Education) to prepare the next generation of AI-infused cybersecurity professionals given the current slate of educational programs available? This not only includes Cyber-AI professional preparation; but also meets the needs of “soft skills” that will be needed by a modern workforce irrespective of industry sector or occupational type. Cyber-AI skills are needed by all in U.S. education and the workforce (both public and private)

# Introduction and Context

6. Guidance and advice to K-12 and Higher Education Institutions on the effective utilization of AI to protect and defend critical campus infrastructure, networks and tech resources; while maximizing opportunities for collaboration, communication, and innovation for students, faculty, and staff. Both red team and blue team members must fully understand the many direct and indirect ways that AI is impacting our security posture, particularly on K-12 and Higher Education Institutions.

7. Given the significant implications for the future of a converged Cyber-AI professional workforce, we introduce a new work role that reflects this reality in the security ecosystem. Thus, one purpose of this paper is to put forth a new work role here that includes a converged AI- Cyber stacking curriculum framework at all levels of the career ladder (Entry-level, Intermediate, Advanced, and Executive levels). We describe a curriculum strategy, structure, and framework in this report to support future AI converged work roles (Section 3).

### Project Scope

Convergence means that AI and Cybersecurity technology are growing together in many significant ways (and at a breathtaking pace). AI is evolving and maturing daily, and the impact and value of securing AI are growing substantially as well. Cybersecurity is also a dynamic field, and AI is further fueling cybersecurity challenges to blue teams and providing potential opportunities for red team malicious actors (both State Actors and Non-State Actors).

We need to build and support a framework that meets the education and workforce needs of key partners and major stakeholders in the complex domain of AI and Cybersecurity. The convergence of AI and Cybersecurity signifies that the professional field (both public and private sectors) must work closer together with K-12 and Higher Education to clearly articulate national strategy and coordinate operational factors into a cohesive and feasible plan for Cyber-AI workforce development and education. This includes tools, tactics, best practices, use cases, and preparation pathways to enhance national Cyber-AI policy and posture.

Thus, the scope of this white paper is to better understand AI-Cybersecurity convergence to design, develop, and implement comprehensive Cyber-AI Education and Workforce Development vision, strategy, and preparation practices to meet current and future critical national needs. Once we have completed this aspect of the white paper scope, we will provide recommendations and strategic actions to enhance Cyber-AI workforce preparation and education programs to reduce critical risks, attack surfaces, and vulnerabilities currently existing within this domain.

If AI-Cybersecurity is the key to the future, there is no time like the present to get started on this white paper and the preparation of the next generation of these emerging tech professionals. This includes increasing K-12 and Higher Education capacity for teachers, faculty, students, and staff across the national, state, and local levels.

# Introduction and Context

## White Paper Key Themes

There are many complex subjects at hand and discussed in this report. The following are key themes that are found throughout the report.

1. The lightning fast speed of innovation in emerging technologies like AI & cybersecurity
2. AI's Impact on reshaping Cybersecurity Education and Workforce Preparation
3. Cyber-AI safety, security, and ethical considerations
4. Key partner and major stakeholder engagement
5. Industry (Public/Private) connections with Academia
6. Federal & State Laws/Legislation/Policy related to Cyber-AI WDE
7. Intro- K-12/Higher Ed/WD/ AI-Cybersecurity Preparedness

## Paper Organization and Structure

There are a variety of pressing issues discussed in this white paper. One primary report purpose is to discuss, analyze, and evaluate AI and Cybersecurity given the convergence processes in progress and the resulting consequences and implications of these national trends. Transformative tech changes are significantly impacting national education and workforce development preparation and best-practices. This policy area is very complex, and dynamic given the quick speed of evolution in AI, Cybersecurity, and their advancing convergence.  Specific policy areas contained within this report are discussed below. In addition, we provide a series of feasible recommendations to support policy and decision makers on specific ways to enhance this critical subject of cybersecurity as impacted by the AI era.

Advancing Cyber-AI in K-12 Education (Section 1)
Advancing Cyber-AI in Higher Education (Section 2)
Cyber-AI Convergence in Workforce Development (Section 3)
Campus Security Practitioner Point of View (Section 4)
AI Legislation, Governance, and Oversight (Section 5)

# Section 1- Advancing AI in K-12 Education: Instruction, Ethics, and Community Collaboration

Section Lead- Dr. Charles Gardner, EnterpriseKC

### Author's Perspective

As Director of the Heartland Cyber Range at EnterpriseKC (EKC), I work at the intersection of curriculum development, technical training, and workforce readiness in the Kansas and Western Missouri region. Prior to this role, I spent ten years with CYBER.ORG, where I led K–12 educator training initiatives, authored national cybersecurity curriculum, and helped build a network of over 40,000 teachers across the United States. These experiences, spanning classroom practice, educator support, and workforce alignment, influence the lens through which I approach this chapter. What follows is a roadmap for advancing AI and cybersecurity education in K–12 settings, with an emphasis on instruction, ethics, and community collaboration that prepares students not just for today's classrooms, but for tomorrow's careers.

## Curriculum Design and Integration

### Grade-Appropriate Curriculum Development

Developing grade-appropriate AI and cybersecurity curricula involves tailoring content to students' cognitive and developmental stages, ensuring foundational concepts are introduced in early grades while progressively building toward advanced topics in critical thinking, data literacy, ethical considerations, and understanding bias in AI systems by high school. While there are many groups and organizations that are doing exceptional work in the area of AI-focused curriculum development, these four stand out as model opportunities for primary and secondary education examples: the AI4K12 Initiative, Impact.AI: K-12 AI Literacy, University of Florida's AI for K-12 Program, and UNESCO's Guidance on AI in Education. It's important to note that not all K-12 AI initiatives, including those listed here, are providing curriculum. Some are merely providing frameworks or insights into effective curriculum development and even professional development opportunities for teachers to learn about how students can learn about (and with) AI.

The AI4K12 initiative, sponsored by the Association for the Advancement of Artificial Intelligence (AAAI) and the Computer Science Teachers Association (CSTA), has developed national guidelines for AI education in K-12. The guidelines are organized around five "Big Ideas" in AI: Perception, Representation & Reasoning, Learning, Natural Interaction, and Societal Impact (AI4K12, 2020). These concepts are structured across four grade bands, providing a scaffolded approach to AI education that introduces age-appropriate content and skills at each educational level.

# Section 1- Advancing AI in K-12 Education: Instruction, Ethics, and Community Collaboration

Developed by the MIT Media Lab, Impact.AI focuses on creating AI curricula and educational platforms that support K-12 students in becoming "technosocial" change agents. The program emphasizes an AI literacy framework covering concepts, practices, and perspectives aligned with this identity. It informs the development of middle school AI curricula, empowering students to become conscious consumers, ethical engineers, and informed advocates of AI (MIT Media Lab, 2024a).

The University of Florida has been instrumental in designing the framework for Florida's public-school AI coursework. Their approach includes specifying course descriptions, learning standards, and benchmarks, ensuring that state learning standards are met, especially in computer science. The program outlines courses that a student needs to earn a certificate or credential and establishes standards for K-12 teachers to meet Florida Department of Education certification to teach AI (University of Florida, 2024).

Also in Florida, for example, state-level efforts are underway to revise Applied Cybersecurity curriculum to include cloud computing, Internet of Things (IoT) IoT, and AI topics while aligning with industry certifications such as CompTIA Security+ and Network+. These revisions are paired with advanced coursework, capstone community projects, and optional offerings like the new Advanced Placement (AP) Cybersecurity course (H. Abrantes, personal communication, December 28, 2024).

UNESCO emphasizes the importance of integrating AI into education systems to prepare students for future challenges. They advocate for curricula that are responsive to the evolving technological landscape, ensuring that students acquire relevant skills and knowledge. This includes fostering an understanding of AI's societal impacts and ethical considerations (UNESCO, 2021).

The research published by Chiu (2021), offers a valuable framework for creating grade-appropriate AI curricula. Through thematic analysis of teacher input, Chiu identifies six essential components for effective curriculum design: AI knowledge, AI processes, the impact of AI, relevance to students, teacher-student communication, and curricular flexibility. By focusing on these components, educators can ensure that AI education remains practical, engaging, and adaptable to the diverse needs of K-12 learners. This approach complements the efforts of larger initiatives like AI4K12 and UNESCO, offering actionable strategies for tailoring AI curricula to different developmental stages.

# Section 1- Advancing AI in K-12 Education: Instruction, Ethics, and Community Collaboration

These frameworks also provide helpful guidance for aligning instruction to grade-level readiness. A practical progression might include:

- Elementary School (K–5): Introduce basic digital citizenship, pattern recognition, and simple discussions around what AI is.
- Middle School (6–8): Explore how data is used in decision-making, basic algorithms, ethical questions (like bias), and foundational cybersecurity topics.
- High School (9–12): Engage in deeper exploration of AI tools, machine learning, real-world cybersecurity scenarios, and ethical dilemmas, ideally culminating in project-based work or early credentialing opportunities.

Clearly aligning AI content with developmental milestones ensures students encounter these critical topics early and often, in ways that are both age-appropriate and future-facing.

### Cross-disciplinary Integration

Cross-Disciplinary integration in K-12 AI education is a promising approach to enrich learning by connecting AI concepts with diverse subject areas. By embedding AI into established disciplines such as computational thinking in math, ethical discussions in social studies, creativity in art, and problem-solving in science, students can experience a well-rounded educational journey that demonstrates the relevance of AI in various fields.

**Science:** Students can employ machine learning models to study and predict complex systems, such as weather patterns or climate change impacts. Resources like National Oceanic and Atmospheric Administration (NOAA) Center for Artificial Intelligence provide tools and data for such explorations, enabling learners to apply AI to environmental science issues effectively (NOAA, 2024). Tools like Google's Earth Engine allow students to analyze satellite data on environmental changes, such as deforestation or water quality, providing a practical connection between AI and real-world environmental challenges.

Building on this, the NSF-funded STELAR initiative emphasizes the value of culturally relevant, project-based AI learning in science classrooms. This approach not only engages students with meaningful projects but also ensures inclusivity by reflecting the diverse contexts and communities they represent. More specific examples of culturally relevant AI learning in STEM education will be explored in the next section. Such methods, combined with advanced AI tools like OpenAI's Codex for creating AI-assisted solutions, empower students to innovate and address sustainability challenges through data-driven approaches.

# Section 1- Advancing AI in K-12 Education: Instruction, Ethics, and Community Collaboration

**Mathematics:** Mathematics provides a crucial foundation for understanding artificial intelligence (AI), particularly through data handling and visualization. Engaging students with real-world datasets using tools like the Common Online Data Analysis Platform (CODAP) allows them to explore and interpret data effectively. CODAP is a free, web-based application designed to support students in learning and performing data science, making it an accessible resource for educational settings (Concord Consortium, 2024).

Additionally, interactive AI applications such as Google's "Quick, Draw!" offer students insights into how AI algorithms process and interpret visual information. In this game, players draw an object, and a neural network attempts to guess the drawing, demonstrating AI's pattern recognition capabilities in an engaging manner (Google, 2024).

By integrating these tools into the curriculum, educators can help students understand AI's role in data science and its applications in analyzing and visualizing data. This approach not only enhances mathematical proficiency but also fosters critical thinking about the ethical and societal implications of AI technologies.

**Arts:** AI in arts can inspire creativity and critical thinking. Tools for digital art creation powered by AI allow students to delve into the interplay between technology and traditional artistic practices. Guided discussions on the societal and philosophical implications of AI in art, informed by resources such as Phys.Org's articles, can foster meaningful, long-term engagement in learning (McMaster, 2024).

**Social Studies:** AI's influence on societal norms, legal frameworks, and policymaking can be a focal point in social studies. For instance, Peter Paccone's work demonstrates how AI tools can be incorporated into lessons to enhance students' understanding of historical and contemporary societal changes, encouraging critical analysis of AI's ethical and social dimensions (Paccone, 2024). An innovative example from Broward County, Florida, involves a collaborative unit between cybersecurity and law students to study the legal dimensions of cybersecurity, including laws like CFAA, HIPAA, and GDPR. This interdisciplinary project not only deepens content knowledge but also inspires new career interests across both domains (H. Abrantes, personal communication, December 28, 2024).

By integrating AI into these diverse fields, K-12 education not only provides students with technical skills but also fosters interdisciplinary connections and critical thinking, preparing them for an AI-infused world.

# Section 1- Advancing AI in K-12 Education: Instruction, Ethics, and Community Collaboration

The potential for AI and cybersecurity integration extends across the entire K–12 curriculum. While this section highlights core academic disciplines, virtually every subject area—including physical education, world languages, and career and technical education—can benefit from the infusion of AI concepts and digital ethics. These efforts are particularly aligned with STE(A)M education, where interdisciplinary problem-solving, creativity, and real-world relevance are already foundational. Additionally, AI and cybersecurity curriculum integration supports pathways outlined in NSA/DHS Centers of Academic Excellence (CAE) programs, helping align secondary education with nationally recognized postsecondary and workforce preparation frameworks. By embracing AI across disciplines, schools not only promote engagement but also prepare students for the cross-functional demands of an AI-infused future.

### Real-World Application Projects

Real-world application projects immerse students in practical, hands-on learning experiences that bridge technology with societal issues. These projects encourage students to use AI and cybersecurity tools to address challenges relevant to their communities, fostering engagement, critical thinking, and a sense of social responsibility. By integrating culturally relevant scenarios and standards such as Learning for Justice's Social Justice Standards, educators can ensure these projects are both meaningful and inclusive (AI for Education, 2023; NIST, 2023).

Key tools and platforms can enhance the accessibility and efficacy of these projects. For instance, TensorFlow, a free open-source AI library, enables students to build and train machine learning models either locally or through cloud-based platforms, where additional hosting costs may apply (AIClub, 2021). Similarly, Google CoLab allows students to experiment with AI in an online environment without requiring local installations, providing an accessible entry point for schools with limited technical resources (AIClub, 2021). These tools empower educators to guide students in exploring real-world AI applications such as environmental monitoring, data analysis, or social equity modeling.

Projects can also leverage frameworks like the NSF-funded STELAR initiative, which integrates culturally relevant, project-based AI learning into high school STEM education. By engaging students in hands-on projects connected to their lived experiences, such as mapping food deserts in urban neighborhoods or analyzing patterns of public transportation accessibility, educators can empower students to address issues deeply rooted in their communities. The STELAR initiative highlights how tailoring education to students' cultural and societal contexts fosters greater engagement and relevance in underserved areas (STELAR, 2024).

# Section 1- Advancing AI in K-12 Education: Instruction, Ethics, and Community Collaboration

For example, educators might use STELAR methodologies to guide students in creating AI models that evaluate equitable access to healthcare services or identify patterns of environmental injustice, such as disproportionate air pollution in marginalized communities. By leveraging tools like TensorFlow for analysis and Google CoLab for collaborative coding, students can explore these pressing issues in meaningful ways. In parallel, culturally relevant cybersecurity projects, such as safeguarding local non-profits from phishing attacks, provide students with opportunities to learn about digital security while giving back to their communities (NIST, 2023).

Other programs explore practical AI solutions with community impact. At Nova High School, AI students work with the Math Department to train teachers in prompt engineering, using AI as a tutoring assistant to improve math learning outcomes (H. Abrantes, personal communication, December 28, 2024). In addition to promoting engagement and community awareness, real-world application projects can serve as a gateway to early workforce experiences. Projects grounded in AI or cybersecurity often mirror entry-level job responsibilities – such as basic data analysis, security auditing, or chatbot development – and can be used to build portfolios or qualify students for internships, apprenticeships, or part-time tech roles after graduation.

By providing access to robust, cost-effective resources and grounding projects in relevant cultural and societal contexts, educators equip students with the skills and awareness to address complex challenges. These real-world applications not only develop technical proficiency but also inspire students to use their knowledge as agents of positive change.

### AI Learning Platforms and Tools

AI learning platforms and tools empower educators to deliver engaging, interactive, and accessible instruction, enabling students to experiment with AI models, analyze data, and develop problem-solving skills. By reflecting on tools already introduced and exploring new ones, this section highlights versatile resources to support differentiated and innovative learning experiences in the classroom.

Previously discussed platforms like TensorFlow and Google CoLab offer students hands-on opportunities to develop and test machine learning models. TensorFlow, as an open-source library, allows learners to explore AI concepts locally or through cloud-based environments, often at minimal cost. Google CoLab complements this by providing a browser-based interface where students and educators can collaborate in real-time without extensive technical setup (AIClub, 2021). Together, these tools establish a foundation for AI exploration across various educational contexts.

# Section 1- Advancing AI in K-12 Education: Instruction, Ethics, and Community Collaboration

CODAP (Common Online Data Analysis Platform) provides another essential resource for classroom use. This free, web-based platform enables students to engage with real-world data through interactive visualizations, fostering a deeper understanding of data science principles and their intersection with AI (Concord Consortium, n.d.). Additionally, Tableau offers educators free licenses, along with resources to teach data analysis and visualization, making it an excellent choice for bringing data-driven insights into the classroom (Data is Good, 2023).

Interactive platforms make AI accessible and exciting for students. The University of Florida's "AI for K-12" Program emphasizes creating course descriptions and benchmarks to integrate AI into K-12 classrooms, equipping students with essential skills for the future workforce (University of Florida, 2024). Similarly, the AI4K12 initiative, jointly supported by NSF, Carnegie Mellon, AAAI, and CSTA, organizes AI concepts into the "Five Big Ideas," providing curated resources to help educators integrate AI topics effectively into K-12 education (AI4K12, 2020).

MIT's RAISE project extends this accessibility by integrating AI capabilities into creative coding environments through Scratch extensions. Students can incorporate AI functionalities like speech recognition and object tracking into their projects, fostering creativity and hands-on engagement with AI concepts (MIT RAISE, 2024).

Differentiated learning tools leverage AI to accommodate diverse student needs and abilities. EduGPT, currently in beta and free for educators, offers customizable teaching assistants, lesson planning support, and real-time classroom interaction tools. These features enable educators to create inclusive, personalized learning experiences while minimizing administrative overhead (EduGPT, 2024).

For educators seeking additional tools, Common Sense Education has curated a list of 15 AI-powered classroom tools with information on pricing and suitability for diverse educational needs. These resources range from tools for personalized learning to platforms for gamified AI education, offering a broad spectrum of possibilities for integrating AI into teaching practices (Common Sense Education, 2024).

# Section 1- Advancing AI in K-12 Education: Instruction, Ethics, and Community Collaboration

By exploring and integrating these platforms, educators can unlock the full potential of AI learning, creating engaging, equitable, and innovative classroom experiences tailored to the needs of their students. However, the impact of these tools depends not just on their availability, but on how they are implemented through effective pedagogy. Educators need support in designing learning experiences that use AI meaningfully – promoting inquiry, ethical reflection, and real-world problem-solving. This also requires strategic collaboration with IT departments and instructional leadership to ensure technologies are deployed securely and sustainably. By aligning teaching practices, technology policies, and classroom innovation, schools can create lasting foundations for AI integration in K–12 education.

As schools explore these platforms, it is essential to recognize how AI can also serve as a tool for expanding access and equity in education. One notable example is Audemy, an AI-driven, audio-based learning environment designed specifically for Blind and Visually Impaired (BVI) students. Audemy uses adaptive technologies to personalize learning experiences through voice interaction, tailoring content based on individual performance, pacing preferences, and engagement levels (Yang & Taele, 2024). Developed in collaboration with accessibility experts and educators, the platform exemplifies how AI can promote inclusive design, remove barriers, and support diverse learners within and beyond traditional classroom settings. These developments underscore the importance of accessibility as a core design principle in K–12 AI implementation.

### Problem-Based and Inquiry-Based Learning

Problem-based and inquiry-based learning (PBL and IBL) immerse students in real-world challenges, fostering critical thinking, collaboration, and a deeper understanding of complex systems. While some studies on PBL focus on advanced fields, such as the use of AI-tutored PBL in medical education (Wu et al., 2020), the core findings are highly relevant to K-12 education. These studies highlight the effectiveness of AI tools in guiding learners through complex, open-ended problems, promoting deeper engagement and practical skill development. By adapting these insights to age-appropriate contexts, educators can leverage similar methods to introduce AI concepts in K-12 classrooms.

A promising direction in AI-assisted pedagogy involves using AI as a "teachable agent" to support student-centered learning. In a recent study, Chen et al. (2024) examined the effect of having university students teach programming concepts to ChatGPT, rather than simply receiving instruction from it. The findings showed that students who engaged in this "learning-by-teaching" method experienced significantly greater gains in programming proficiency and Self-Regulated Learning (SRL) strategies than those who learned through traditional video instruction. While both groups improved, the ChatGPT-enabled learners were notably stronger in writing readable and logically sound code. The study emphasized that the value of teachable

AI agents lies not just in their accuracy but in the learning processes they stimulate. Designing tasks where students must challenge or correct AI responses—such as identifying mistakes or improving upon ChatGPT's output—can enhance critical thinking, ethics, and self-efficacy. These findings offer a compelling model for K-12 educators seeking to deepen engagement in PBL environments by encouraging students to actively interrogate and guide AI-generated content.

Tools such as PRIMARYAI (Lee et al., 2021) exemplify how AI-infused PBL can be tailored to younger students. This game-based learning environment allows upper elementary students to tackle life science problems, like investigating ecosystem changes, through AI-supported inquiry. Similarly, Teachable Machine by Google (2024) empowers students to create and train their own machine learning models, enabling hands-on exploration of AI's practical applications. Platforms like Cognii, while not free, offer AI-driven, open-response tutoring systems to guide inquiry projects, fostering collaboration and personalized learning experiences (Cognii, 2024). These tools collectively demonstrate how PBL and IBL methodologies can integrate AI concepts effectively into K-12 education.

By embedding AI into inquiry and problem-based frameworks, educators not only teach technical skills but also prepare students to approach complex, real-world challenges with creativity and ethical awareness. This foundation supports the broader goals of digital citizenship and lifelong learning, connecting seamlessly with the upcoming discussions on ethics and teacher upskilling.

### Teacher Training and Upskilling

Effective implementation of AI education relies on comprehensive teacher training and upskilling programs that equip educators with the knowledge, tools, and confidence to integrate emerging technologies into the classroom. These programs address both technical understanding and pedagogical strategies, fostering an environment of continuous learning and innovation.

Educators often find topics like artificial intelligence and cybersecurity daunting due to their technical complexity and unfamiliarity. The National Security Agency's (NSA) GenCyber program, while primarily focused on cybersecurity, serves as a compelling model for how targeted Professional Development (PD) can empower teachers to master advanced content and integrate it into interdisciplinary classrooms. By aligning teacher training with GenCyber's Cybersecurity First Principles, participants gained practical skills and confidence to introduce foundational cybersecurity concepts to students (NSA, 2024). The success of these programs underscores the importance of structured, supportive PD and serves as a parallel for AI-focused teacher training initiatives. Programs like the MIT Media Lab's RAISE Initiative provide a strong foundation for equipping teachers to bring AI concepts into K-12 classrooms. Through offerings like the "Day of AI" and teacher-focused workshops, RAISE emphasizes responsible AI use while delivering actionable resources for classroom integration (MIT Media Lab, 2024b). Similarly, platforms like

# Section 1- Advancing AI in K-12 Education: Instruction, Ethics, and Community Collaboration

EdTechTeacher offer robust professional development opportunities through their membership and live course models, providing educators with in-depth training on AI tools and strategies for application in real-world teaching. The EdTechTeacher membership, which costs $195 annually, can be shared by schools or districts to make the investment more accessible (EdTechTeacher, 2024).

Another example is Parallax Inc., which combines free AI-focused curriculum and professional development for teachers with hands-on activities using affordable micro:bit devices. Teachers can guide students in building chatbots and exploring robotics through Python programming, making AI accessible and engaging for learners of all backgrounds (Parallax Inc., 2023).

**Demonstrating Success:** The RAICA Study. A study on MIT's RAICA (Responsible AI for Computational Action) curriculum provides a concrete example of success in AI teacher training. Teachers who participated in the RAICA PD programs reported increased confidence in introducing AI concepts to students, heightened awareness of AI's societal impacts, and improved interdisciplinary teaching strategies. The findings demonstrate how focused PD can empower educators to effectively integrate AI into their classrooms while addressing ethical and societal considerations (RAICA, 2024).

By drawing from other effective PD models like GenCyber and leveraging resources such as Parallax, RAISE, and EdTechTeacher, schools can ensure that educators are equipped to meet the demands of AI education. Structured training programs that provide technical knowledge, ethical frameworks, and practical tools prepare teachers to engage students in meaningful AI learning experiences. With comprehensive support, teachers can overcome initial apprehension and confidently incorporate AI into their instructional models, fostering student success in an AI-driven world. In Florida, the University of Florida's EQuIPD program (Engaged Quality Instruction through Professional Development) is playing a vital role in helping teachers incorporate AI and related technologies into K–12 instruction. The program blends professional learning, real-world applications, and emerging tools like AI and drones to boost both educator confidence and student outcomes, especially in STEM-related fields (University of Florida, 2025). This approach is directly influencing how school districts update their CTE pathways.

For example, in Broward County Public Schools, efforts are underway to align curriculum with foundational AI, cybersecurity, and cloud computing concepts, while integrating industry certifications and community-relevant capstone projects (H. Abrantes, personal communication, December 28, 2024)

# Section 1- Advancing AI in K-12 Education: Instruction, Ethics, and Community Collaboration

### Safety, Security, and Ethical Considerations

### Student Data Privacy and Safety

Protecting student data privacy and safety in AI and cybersecurity education requires practical, achievable steps for schools to adopt secure technologies and implement policies, empowering educators and administrators with accessible tools, clear guidelines, and professional development to create a safe digital environment for learning.

As AI tools become more prevalent in K–12 classrooms, safeguarding student information must be a foundational priority. Many AI platforms rely on data collection to personalize learning, adapt assessments, or improve user experience—but without strong data governance practices, these benefits can come at the cost of student privacy. Common risks include unauthorized data sharing, unintentional exposure of Personally Identifiable Information (PII), and insufficient oversight of third-party educational tools (U.S. Department of Education, 2014; Future of Privacy Forum, 2023).

School districts are beginning to respond with stricter internal guidelines and vetting procedures. For example, Broward County Public Schools (BCPS) in Florida maintains stringent data privacy protocols for adoption of classroom technology, ensuring alignment with district policy before any platform is approved for use (H. Abrantes, personal communication, December 28, 2024). These local efforts mirror broader national recommendations from organizations like the U.S. Department of Education's Student Privacy Policy Office and the Consortium for School Networking (CoSN), which stress transparency, parental consent, and clearly defined data retention practices when integrating AI-powered technologies in education (U.S. Department of Education, 2014; CoSN, 2023).

Equally important is professional development for educators and administrators. Many teachers are enthusiastic about using AI tools but lack the training to evaluate them from a privacy or security standpoint. Providing guidance on interpreting Terms of Service, enabling privacy settings, and selecting FERPA-compliant platforms is essential for classroom-level implementation. Resources like Common Sense Education's privacy evaluation rubrics and CoSN's toolkit for data governance help bridge this gap by offering ready-to-use frameworks for school leaders (Common Sense Education, 2024; CoSN, 2023).

Ultimately, prioritizing student data privacy is not a barrier to innovation—it's a critical enabler. When educators are empowered to make informed, secure choices about the tools they use, schools can confidently leverage AI's potential without compromising student trust or safety.

# Section 1- Advancing AI in K-12 Education: Instruction, Ethics, and Community Collaboration

### Ethics and Digital Citizenship

Ethics and digital citizenship education evolves throughout a student's K–12 journey, beginning with foundational lessons on online safety and respect for others, progressing to critical analysis of bias and ethical dilemmas in technology during middle school, and culminating in high school with real-world applications and responsible decision-making as students prepare to navigate the complexities of an increasingly digital world.

In the early grades, digital citizenship starts with understanding personal responsibility online—such as protecting login credentials, avoiding cyberbullying, and evaluating basic digital content. As students mature, instruction expands to include broader ethical issues such as algorithmic bias, misinformation, data manipulation, and the social consequences of automated decision-making. Organizations like Common Sense Education have developed grade-banded curricula to scaffold these topics, providing resources on digital footprint awareness, media balance, and responsible technology use across K–12 (Common Sense Education, 2024).

By middle and high school, students are more capable of engaging with complex ethical frameworks related to artificial intelligence and cybersecurity. The MIT RAISE initiative (Responsible AI for Social Empowerment and Education) emphasizes age-appropriate conversations around algorithmic fairness, data privacy, and unintended consequences of AI systems. Through creative tools like Scratch extensions, students can explore AI while reflecting on its societal impacts (MIT Media Lab, 2024b). The RAICA study (Responsible AI for Computational Action) further reinforces the importance of teaching ethics through interdisciplinary activities, helping educators blend technical instruction with moral reasoning (RAICA, 2024).

Real-world service-learning applications help students internalize these lessons. At Nova High School in Florida, cybersecurity students partnered with a local assisted living facility to deliver digital literacy and online safety workshops to elderly residents—an experience that strengthened both ethical reflection and community ties (H. Abrantes, personal communication, December 28, 2024). This type of outreach reinforces the principle that ethical technology use isn't just a personal issue—it's a civic responsibility.

Digital citizenship is also tied closely to the responsible use of generative AI tools in the classroom. With the rise of AI-assisted writing, media generation, and data analysis, students must be taught to critically assess sources, disclose AI assistance when appropriate, and understand the risks of misrepresentation or overreliance on automated systems. Ethical instruction must now include not only how students behave online, but how they interact with increasingly autonomous systems.

# Section 1- Advancing AI in K-12 Education: Instruction, Ethics, and Community Collaboration

By embedding ethics and digital citizenship across grade levels—and linking them to real-world experiences—schools prepare students to navigate an AI-infused society with integrity, empathy, and a sense of shared responsibility.

## Collaborative Engagement with Stakeholders

### Role of Parents, Families, and Guardians

Parents, families, and guardians play a critical role in supporting AI and cybersecurity education by fostering curiosity and partnering with schools, while also engaging in their own learning about responsible technology use to better guide students in developing the skills and ethics needed to navigate the digital world safely and confidently.

In the context of AI and cybersecurity, the home environment significantly shapes students' attitudes, behaviors, and digital habits. Parents are often the first line of defense in conversations about online safety, privacy, and appropriate use of technology. Yet, research consistently shows that many families feel underprepared to engage with emerging technologies like artificial intelligence. Surveys by Pew Research Center and others reveal growing concern among parents about their children's interactions with AI-powered tools—ranging from chatbots to smart home devices—but also a lack of clear guidance on how to manage them (Auxier et al., 2022).

To bridge this gap, schools must treat families not as passive recipients of information but as active partners in the learning process. Open houses, family tech nights, and parent-focused webinars are increasingly used to introduce families to the AI and cybersecurity concepts their students are learning. At Nova High School in Florida, for example, school leaders host open house events to introduce families to the school's AI and cybersecurity programs. These efforts not only build awareness but also foster stronger relationships between educators and families, helping drive enrollment and enthusiasm for the program (H. Abrantes, personal communication, December 28, 2024).

Several national organizations have developed free resources to help parents build their own digital literacy. Common Sense Media offers AI explainers, conversation guides, and parent-specific toolkits designed to demystify technologies and promote safe, informed engagement at home (Common Sense Media, 2024). Similarly, Cyber.org provides family-friendly materials focused on cybersecurity awareness, such as activities that teach secure password creation, data sharing risks, and ethical digital behavior (Cyber.org, 2024).

# Section 1- Advancing AI in K-12 Education: Instruction, Ethics, and Community Collaboration

Ultimately, family engagement is not about mastering the latest tech jargon—it's about modeling curiosity, responsibility, and adaptability. When parents ask thoughtful questions, explore tools alongside their children, and acknowledge the ethical challenges that AI can introduce, they help create a culture of learning that extends beyond the classroom. Empowering families to grow alongside their students is essential to creating a community of responsible digital citizens.

### School and District Leadership

School and district leadership is essential for driving AI and cybersecurity education by establishing clear priorities, allocating resources for teacher training and technology, and fostering a culture of innovation and ethical responsibility that prepares students for the challenges of a digital future.

The successful integration of AI and cybersecurity into K–12 education depends heavily on proactive, informed leadership at both the school and district levels. Administrators are uniquely positioned to set the tone for innovation by shaping policies, prioritizing strategic investments, and supporting professional development opportunities for staff. Without such top-down commitment, even the most ambitious classroom efforts may struggle to gain traction or scale effectively.

Visionary leadership begins with establishing a shared understanding of what AI and cybersecurity education should look like in practice. This includes defining clear goals, aligning with national frameworks like the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and ensuring all technology use complies with federal and state privacy laws (NIST, 2023). At the same time, leaders must support curriculum development that is responsive to both local needs and emerging technologies. In Florida's Broward County Public Schools, for instance, collaboration between school administrators and the district's Career Technical and Community Education (CTACE) office has been instrumental in supporting innovative AI and cybersecurity programs at Nova High School (H. Abrantes, personal communication, December 28, 2024).

Regionally, organizations like EnterpriseKC (EKC) play a valuable role in supporting school and district leadership by convening educators, employers, and policymakers around a shared vision for AI and cybersecurity education. EKC has helped facilitate strategic alignment across institutions, enabling schools to better navigate resource constraints and connect with workforce initiatives in meaningful ways (EnterpriseKC, 2024).

Resource allocation is another critical function of leadership. Districts must ensure schools have access to secure infrastructure, up-to-date hardware, and scalable platforms capable of supporting AI-driven instruction. Equally important is funding for teacher professional development. Leaders who prioritize training—whether through internal workshops, external PD programs, or partnerships with higher education—equip educators to integrate complex content confidently and effectively.

Beyond logistics, school and district leaders play a vital cultural role. By fostering a growth mindset toward emerging technology, modeling ethical decision-making, and encouraging cross-department collaboration, leaders help cultivate a school-wide environment where AI and cybersecurity education can thrive. Initiatives like CoSN's EmpowerED Superintendent Toolkit provide strategies and case studies to help education leaders make informed, equity-driven decisions around AI, digital tools, and data governance (Consortium for School Networking, 2023).

While governance has been implicitly woven throughout this chapter, in discussions of leadership, policy-setting, resource allocation, and stakeholder coordination, it is worth explicitly acknowledging its importance. Governance refers to the structures, policies, and decision-making processes that ensure educational technologies, especially AI and cybersecurity initiatives, align with institutional values, legal standards, and community needs. As schools and districts adopt increasingly complex technologies, governance frameworks are essential to guide implementation, assess risk, ensure equity, and build trust across all stakeholders.

Ultimately, leadership that embraces AI and cybersecurity not as short-term trends but as essential components of modern education ensures that students, teachers, and communities are future-ready. By combining strategic planning, community engagement, and ethical vision, school and district leaders can guide transformative change at scale.

### Partnerships with Industry and Higher Education

Partnerships with industry and higher education institutions provide invaluable resources and expertise to enhance AI and cybersecurity education, offering real-world insights, mentorship opportunities, and access to cutting-edge tools and research that prepare students for future academic and career pathways.

These partnerships bridge the gap between classroom learning and workforce realities, allowing students to engage with current trends, technologies, and professionals who are actively shaping the fields of artificial intelligence and cybersecurity. Industry partners can offer guest speakers, internships, mentorship, and access to proprietary platforms or training environments, while higher education institutions often provide dual-enrollment opportunities, curriculum frameworks, or teacher training aligned with state standards and career certifications.

# Section 1- Advancing AI in K-12 Education: Instruction, Ethics, and Community Collaboration

One compelling example comes from Nova High School in Florida, where students benefit from partnerships with TechGateway, a regional initiative that connects local tech companies with K–12 schools to offer insights into how cybersecurity and AI are applied in real-world business contexts (H. Abrantes, personal communication, December 28, 2024). These relationships give students early exposure to the professional landscape and allow educators to design instruction that reflects emerging industry needs.

In the Kansas City region, EKC supports this type of cross-sector collaboration by connecting school districts, higher education institutions, and employers to co-develop and scale programs in AI and cybersecurity. EKC's role as a neutral convener helps create ecosystem alignment, ensuring that students not only learn future-ready skills but also understand how to apply them within their local communities (EnterpriseKC, 2024).

Higher education institutions are equally vital collaborators. The University of Florida's AI for K–12 initiative serves as a statewide model for articulating standards, credentialing teachers, and aligning curriculum with AI literacy objectives and career readiness (University of Florida, 2024). Their collaboration with K–12 schools through the EQuIPD program also empowers teachers to bring AI concepts into the classroom using best practices informed by university research and instructional design.

National efforts like the Mark Cuban Foundation's AI Bootcamps demonstrate how nonprofits and industry can provide free, accessible programming for high school students from underserved communities. These weekend intensives introduce learners to core AI concepts and tools, while also connecting them with mentors working in tech fields (Mark Cuban Foundation, 2024). By partnering with tech companies to host these events, the foundation helps demystify AI while building student confidence and interest in tech careers.

These industry and higher education collaborations are especially critical for expanding early workforce access. By co-developing internship programs, stackable credential pathways, or job-shadowing opportunities, partners can ensure that high school graduates leave with not just knowledge – but resume-ready experiences. In regions like Kansas City, organizations like EKC work to ensure that AI and cybersecurity learning opportunities are directly tied to real job prospects for youth entering the workforce (EnterpriseKC, 2024).

Ultimately, these collaborations not only provide students with tangible career pathways, but they also help schools remain agile and responsive to a rapidly evolving technological landscape. When K–12 institutions, colleges, and companies co-design educational experiences, students benefit from a networked ecosystem that supports both academic exploration and workforce preparation.

## Section 1 Conclusion

Preparing students for the age of AI requires more than a technical curriculum, it demands a rethinking of how we teach, what we teach, and who we involve in the process. As introduced in this chapter, the convergence of artificial intelligence and cybersecurity is not just a workforce issue but a fundamental education challenge that K–12 systems must meet head-on.

Throughout this chapter, we've outlined four core areas where this work must take shape: designing age-appropriate, relevant curriculum; equipping educators with effective tools and methods; safeguarding student data and promoting ethical digital citizenship; and building lasting partnerships with families, schools, and industry. These pillars form a comprehensive foundation for ensuring all students, not just future computer scientists, can meaningfully engage with AI and cybersecurity in their lives and communities.

The call to action is clear: invest in teacher support, elevate digital ethics, open doors to industry, and treat K–12 learners as the next generation of not just users, but builders of intelligent systems. If we get this right, we will not only close skills gaps, we will open up a future where all students are empowered to lead, create, and thrive.

## References

AI for Education. (2023). Integrate social justice standards. Retrieved from https://www.aiforeducation.io/prompts/integrate-social-justice-standards

AI4K12. (2020). Sparking curiosity in AI. Retrieved from https://ai4k12.org/

AIClub. (2021, August 26). TensorFlow for high school projects. Retrieved from https://corp.aiclub.world/post/tensorflow-for-high-school-projects

Auxier, B., Rainie, L., & Anderson, M. (2022). AI and the future of learning: Parental concerns in the age of smart tech. Pew Research Center. Retrieved from https://www.pewresearch.org/

Chen, A., Wei, Y., Le, H., & Zhang, Y. (December, 2024). Learning-by-Teaching with ChatGPT: The Effect of Teachable ChatGPT Agent on Programming Education. arXiv preprint arXiv:2412.15226. Retrieved from https://arxiv.org/abs/2412.15226

# References

Chiu, T. K. F. (2021, August 12). A holistic approach to the design of artificial intelligence (AI) education for K-12 schools. TechTrends, 65(5), 796–807. Retrieved from https://link.springer.com/article/10.1007/s11528-021-00637-1

Cognii. (2024). K-12 AI education solutions. Retrieved from https://www.cognii.com/solutions#k-12

Common Sense Education. (2024). Classroom tools that use AI. Retrieved from https://www.commonsense.org/education/lists/classroom-tools-that-use-ai

Common Sense Education. (2024). Digital citizenship curriculum. Retrieved from https://www.commonsense.org/education/digital-citizenship

Common Sense Education. (2024). Privacy evaluations for educational technology. Retrieved from https://privacy.commonsense.org/

Common Sense Media. (2024). AI and your child: A guide for parents. Retrieved from https://www.commonsensemedia.org/

Concord Consortium. (2024). CODAP: Common Online Data Analysis Platform. Retrieved from https://codap.concord.org

Consortium for School Networking. (2023). EmpowerED Superintendent Toolkit. Retrieved from https://cosn.org/toolkits/

Consortium for School Networking. (2023). Protecting privacy in connected learning: A toolkit for schools. Retrieved from https://cosn.org/privacy/

Cyber.org. (2024). Family cybersecurity resources. Retrieved from https://www.cyber.org/

Data is Good. (2023, May 18). Tableau in education: How to use Tableau in the classroom.

Retrieved from https://dataisgood.com/tableau-in-education-how-to-use-tableau-in-classroom/

Drozda, Z. (2024). Executive Director, Data Science 4 Everyone. Data Science 4 Everyone.

Retrieved from https://www.datascience4everyone.org/post/ds4e-invited-to-the-white-house-discusses-ai-education

EdTechTeacher. (2024). AI for teachers. Retrieved from https://edtechteacher.org/ai-for-teachers/

EduGPT. (2024). EduGPT for educators. Retrieved from https://edugpt.com

# References

EnterpriseKC. (2024). About EKC. Retrieved from https://enterprisekc.com/

Future of Privacy Forum. (2023). Student privacy and edtech: Navigating emerging technologies in the classroom. Retrieved from https://fpf.org/issues/k-12-education/

Google. (2024). Quick, Draw!. Retrieved from https://quickdraw.withgoogle.com

Google. (2024). Teachable Machine. Retrieved from https://teachablemachine.withgoogle.com/

Lee, S., Mott, B., Ottenbreit-Leftwich, A., Scribner, A., Taylor, S., Park, K., Rowe, J., Glazewski, K., Hmelo-Silver, C. E., & Lester, J. (2021). AI-infused collaborative inquiry in upper elementary school: A game-based learning approach. Proceedings of the Thirty-Fifth AAAI Conference on Artificial Intelligence.

Mark Cuban Foundation. (2024). AI Bootcamps. Retrieved from https://www.markcubanai.org/
McMaster, G. (2024, February 20). AI Art Generators Have a Place in K-12 Classrooms, Say Researchers. Phys.Org. Retrieved from https://phys.org/news/2024-02-ai-art-generators-classrooms.html

Miao, F. (2024). Chief of Unit for Technology and Artificial Intelligence in Education, UNESCO. WISE Qatar. Retrieved from https://www.wise-qatar.org/biography/fengchun-miao/

MIT Media Lab. (2024a). Impact.AI: K-12 AI Literacy. Retrieved from https://www.media.mit.edu/projects/impact-ai-k-12/overview/

MIT Media Lab. (2024b). RAISE: Responsible AI for social empowerment and education. Retrieved from https://www.media.mit.edu/articles/raise-resources/

MIT RAISE. (2024). Creativity with Scratch and AI. Retrieved from https://raise.mit.edu/research-projects/creativity-with-scratch-and-ai/

National Institute of Standards and Technology (NIST). (2023). The cyber range: A guide. Retrieved from https://www.nist.gov/document/cyber-range

National Institute of Standards and Technology (NIST). (2023). Cybersecurity Framework: Implementation guidance for K–12 education. Retrieved from https://www.nist.gov/cyberframework

National Oceanic and Atmospheric Administration (NOAA). (2024). NOAA Center for Artificial Intelligence (NCAI). Retrieved from https://www.noaa.gov/ai

National Security Agency (NSA). (2024). GenCyber: Cybersecurity camps for educators and students. Retrieved from https://www.nsa.gov/resources/educators/gen-cyber/

# References

Paccone, P. (2024, September 11). Enhancing History Education: The AI Advantage in K-12 Education. Retrieved from https://ncheteach.org/blog/webinar/enhancing-history-education-the-ai-advantage-in-k-12-education/

Parallax Inc. (2023). Introducing our new artificial intelligence tutorial series with Python and micro:bit. Retrieved from https://www.parallax.com/introducing-our-new-artificial-intelligence-tutorial-series-with-python-and-microbit/

Responsible AI for Computational Action (RAICA). (2024). RAICA curriculum study: Teacher perspectives on AI education. Retrieved from https://arxiv.org/abs/2312.04839

STELAR. (2024). Integrating culturally relevant project-based AI learning in high school STEM education. Retrieved from https://stelar.edc.org/projects/24645/profile/integrating-culturally-relevant-project-based-ai-learning-high-school-stem

TeachAI. (2024). Retrieved from https://www.teachai.org/

U.S. Department of Education. (2014). Protecting student privacy while using online educational services: Requirements and best practices. Retrieved from https://studentprivacy.ed.gov/

UNESCO. (2021). Artificial Intelligence and Education: Guidance for Policy-makers. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000380602

University of Florida. (2024). AI for K-12. Retrieved from https://ai.ufl.edu/about/ai-for-k-12/

University of Florida. (2025, May 1). Drones, AI help Florida farmers save money and water. Retrieved from https://news.ufl.edu/2025/05/drones-ai-help-farmers-save-money/

Wu, R., Liu, H., Lin, Y., & Chang, Y. (2020). Artificial intelligence-tutoring problem-based learning in ophthalmology clerkship. Annals of Translational Medicine, 8(12), 737. Retrieved from https://atm.amegroups.com/article/view/33749/html

Yang, C., & Taele, P. (2025, April 23). AI for accessible education: Personalized audio-based learning for blind students. arXiv. https://arxiv.org/abs/2504.17117

# References

Paccone, P. (2024, September 11). Enhancing History Education: The AI Advantage in K-12 Education. Retrieved from https://ncheteach.org/blog/webinar/enhancing-history-education-the-ai-advantage-in-k-12-education/

Parallax Inc. (2023). Introducing our new artificial intelligence tutorial series with Python and micro:bit. Retrieved from https://www.parallax.com/introducing-our-new-artificial-intelligence-tutorial-series-with-python-and-microbit/

Responsible AI for Computational Action (RAICA). (2024). RAICA curriculum study: Teacher perspectives on AI education. Retrieved from https://arxiv.org/abs/2312.04839

STELAR. (2024). Integrating culturally relevant project-based AI learning in high school STEM education. Retrieved from https://stelar.edc.org/projects/24645/profile/integrating-culturally-relevant-project-based-ai-learning-high-school-stem

TeachAI. (2024). Retrieved from https://www.teachai.org/

U.S. Department of Education. (2014). Protecting student privacy while using online educational services: Requirements and best practices. Retrieved from https://studentprivacy.ed.gov/

UNESCO. (2021). Artificial Intelligence and Education: Guidance for Policy-makers. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000380602

University of Florida. (2024). AI for K-12. Retrieved from https://ai.ufl.edu/about/ai-for-k-12/

University of Florida. (2025, May 1). Drones, AI help Florida farmers save money and water. Retrieved from https://news.ufl.edu/2025/05/drones-ai-help-farmers-save-money/

Wu, R., Liu, H., Lin, Y., & Chang, Y. (2020). Artificial intelligence-tutoring problem-based learning in ophthalmology clerkship. Annals of Translational Medicine, 8(12), 737. Retrieved from https://atm.amegroups.com/article/view/33749/html

Yang, C., & Taele, P. (2025, April 23). AI for accessible education: Personalized audio-based learning for blind students. arXiv. https://arxiv.org/abs/2504.17117

# Section 2- Advancing AI-Cybersecurity Convergence in Higher Education Curriculum, Pedagogy, Research, and Service

Section Lead- Dr. Keith Clement, Professor, Fresno State University, ATARC Cybersecurity Education and Workforce Development Academic Chair

### Introduction and Linkage to K-12 Education

AI is rapidly changing K-12 Education in numerous and innovative ways. It is impacting education administration, learning/teaching within the classroom, curriculum and standards, how teachers are prepared to teach it, how students use it to learn, and many other ways as previously discussed. AI is transforming global education and ushering in a new paradigm and way of learning and education nationally. The first report Section was an excellent discussion of the ongoing evolution throughout K-12 grades and the varied subject areas using AI effectively to make a difference in student learning and teacher pedagogy and activities. AI is enhancing both Science Technology, Engineering, and Mathematics/Arts (STEM/STEAM) and professional based Career Education Training (CTE) programs, courses, and curriculum. Changes due to AI are found in curriculum and standards design, cross-disciplinary real-world applications and projects, instructional methods and tools, teacher training and upskilling, safety-security-ethical concerns, ethics and digital citizenship, collaborative engagement and stakeholders, school and district leadership, and developing partnerships with industry, academia, and government. Clearly AI is impacting K-12 education.

Section One also discussed the core pillars to form a comprehensive K-12 Education foundation upon which to build upon. The evolution of AI and security education and programs at lower grades in turn impact the administration, teachers, and students in the higher grades. These pillars also serve as a foundational baseline to build upon in coordination with higher education institutions nationally. Given the important dual roles of K-12 for both college readiness and career preparedness, there are significant linkages with Report Section Two (advancing higher education); and the following Section Three on future Cyber-AI converged workforce development preparation. It is vital to ensure a smooth transition from earlier grades, high schools, and on to colleges and universities for interdisciplinary students drawn from all academic majors. This is true, both for students pursuing careers in Cyber-AI domains, but also others looking for careers in a modern workplace. Millions of high school graduates transfer annually to colleges and universities. We must make sure that all of them are provided Cyber-AI literacy, fluency, and experience to succeed within the workplace..

Section Two discusses and analyzes Cyber-AI convergence trends in higher education, their impact/implications, and make related policy recommendations for consideration to enhance American Cyber-AI education and workforce development policy and best practices. We must align and link K-12 and Higher Education AI-Cybersecurity programs, curriculum, standards, teaching pedagogy, instructional materials, labs, hand-on tools/applications to support degree and certificate seekers from all walks of life. AI has created a tremendous change in how schools, colleges, and universities operate. Significant and transformative change will continue to accelerate in coming years as AI implications continue to deepen. AI has impacted and altered the current and future trajectory of learning, teaching, research, and service in schools, colleges, and universities. However, we must also do better to further evolve higher education to prepare our graduates for success in the future digital world including important skill-sets ( both technical and soft skills) to enhance preparation for current and future Cyber-AI workplace (as well as heavily impacting multi-facets of our lives.) As such, higher education and training will continue to evolve significantly given the accelerating trend towards convergence of AI and emerging technologies maturing at lightning speed. This has significant implications when factoring in cybersecurity, networking, and quantum computing in the coming years of the age of AI.

### Cyber-AI Education within Higher Education

While AI is converging technologically across many other sectors and industries, this report is primarily interested in the critical implications with the cybersecurity domain and specific impacts in education and workforce development. The great AI transformation is energetically underway within higher education and the academic community. What is the impact of Cyber-AI convergence on U.S. Higher Education circa 2025? This report section analyzes and evaluates the current impact and future implications of Cyber-AI in higher education and professional preparation in the U.S.

For historical context, computing "thinking" machinery was introduced in 1950 by Alan Turing (mathematician and computer scientist). In 1956, the term "AI" was coined at Dartmouth University. Recent advances in AI were made possible by the last 70 years of innovation and technology in computing (more power, increased memory, and sharper graphics), Graphic User Interface (GUI), development of the World Wide Web (WWW), and the recent proliferation of social media and related digital content. It took a while for each of these tech innovations to spread across society and into the mainstream and consumer electronics. However, has AI completely captured our societal imagination since OpenAI and the release of ChatGPT in 2023. In two very short years, generative AI has surpassed 50 million users and is busy transforming daily aspects of human life and organizational activity. The possibility of continued remarkable transformative growth through agentic (decision-making) and autonomous AI, physical AI (robotics and industrial machines) seems assured. As such, we should expect to see additional issues grow as organizations and individuals continue to deploy and utilize AI amid raising concerns for securing data, systems, networks, and our cyberspace nationwide.

We are interested in convergence trends of AI and Cybersecurity in higher education and how to advance these critical digital literacy, fluency, and necessary skills/tools so important for life in a growing tech savvy society. Prior to discussing the details of AI-Cybersecurity within higher education, we first discuss key terms, convey the large numbers of enrolled students within U.S., and discuss relevant population demographics trends institutions, and lay out the context of Cyber-AI in professional career education and workforce preparation.

Higher Education is defined as the various types of education given in postsecondary education and usually affording degrees, diplomas, or certificates of higher studies; includes universities and colleges, various professional schools such as law, medicine, and business, and teacher-training schools, junior colleges, and institutes of technology. [10] There are many types of higher educational institutions nationwide (below) with Table 1 showing the number of U.S. Title IV Higher Educational Institutions in the 2022-2023 academic year. [11]

**Table #1: Number of Title IV Institutions in the U.S. and Other Jurisdictions (2022-2023)**

2,691 classified as 4-year institutions

1,496 were 2-year institutions

1,632 were less than 2-year institutions

Total- 5,819

Source: https://nces.ed.gov/whatsnew/press_releases/8_21_2024.asp

The numbers of students enrolled in U.S. higher educational institutions is found in Table 2 (below) utilizing data drawn from the Spring 2025 Academic Term by the National Student Clearinghouse Research Center (NSCRC) and summarized by bestcolleges.com. [12] It is important to note the total number colleges and universities has declined since the COVID period (2020-2024). In addition, the anticipated number of students enrolled in higher education institutions will begin to decline in the next few years as we approach the demographic "enrollment cliff" of fewer traditional college-aged students in the population. This issue is currently impacting K-12 education nationwide. Detailed information of the long-expected student enrollment cliff is discussed in further detail below.

The 2025 high school graduation class is the biggest in American history. However, student enrollment numbers will begin to decline year over year for the foreseeable future. As such, in the near term (next 4-5 years), the number of students enrolled in college and universities will continue to increase. However, after that initial boost, higher education institutions will see fewer traditional age college students in colleges and universities. This will place future pressures on

[10] Britannica.com/topic/higher-education Accessed electronically on 9/20/2025.

[11] **https://nces.ed.gov/whatsnew/press_releases/8_21_2024.asp** Accessed electronically on 9/20/2025.

[12] **bestcolleges.com/research/college-enrollment-statistics/** Accessed electronically on 9/20/2025.

# Section 2- Advancing AI-Cybersecurity Convergence in Higher Education Curriculum, Pedagogy, Research, and Service

college and university student enrollment numbers, but also the number of students studying in STEM/STEAM fields related to emerging technologies. Current higher education student enrollments are found in the table below.

**Table #2: Student Enrollment by Degree Level (Spring 2025 Term)**

Associate: 4.4 million students
Bachelors: 8.3 million students
Undergraduate Certificates and Other Non-Degree Programs: 2.1 million students
Masters: 1.8 million students
Professional: 345,000 students
Doctoral: 624,000 students
Graduate Certificates and Other Non-Degree Programs: 119,000 students

Source: bestcolleges.com/research/college-enrollment-statistics/

According to NSCRC estimates, about **18.4 million students** were enrolled at a postsecondary institution, including over 15 million undergraduates and about 3.1 million graduate students. [13] In May 2025 (the end of the spring term), there were approximately **55.0 million K-12** students in the U.S. [14] **With a total of 73.4 million K-12 and Higher Education students in Spring 2025, this is a fantastic opportunity to roll out critical professional preparation skillsets with the emergent technologies and tools they need exposure to through the education and training process.** The U.S. Census Bureau estimates the 2025 U.S. population at 342.7 million people. [15]

Approximately 20% of the population is a K-12 or Higher education student and learner. This figure does not include teachers, faculty, staff, and administrators. We need to make sure we are reaching all students (and faculty/staff) and teaching what they need to know about effective utilization of AI and cybersecurity skills and competencies so they will be properly prepared for future education and workforce success.

At the beginning of 2025, an estimated **54.1 million K-12 students** and 5.7 million teachers will be back at school this fall. [16] In combination with large numbers of K-12 Education students nation-wide, this is a lot of students. As educators, teachers, and professors, we need to make sure all students are properly prepared for current and future AI and Cybersecurity skills and filling available positions. **We should leverage K-12 and Higher Education to prepare all students for the development and utilization of Cyber-AI skills with the broader objective of a wider dispersion of skills and literacy into the greater society down the road.**

[13] **bestcolleges.com/research/college-enrollment-statistics/** Accessed electronically on 9/20/2025..
[14] **https://www.ibisworld.com/united-states/bed/number-of-k-12-students/4251/** Accessed electronically on 10/12/2025.
[15] **https://www.census.gov/** Accessed electronically on 9/20/2025.
[16] **https://www.census.gov/newsroom/stories/back-to-school.html#** Accessed electronically on 10/12/2025.

# Section 2- Advancing AI-Cybersecurity Convergence in Higher Education Curriculum, Pedagogy, Research, and Service

Students learn about Cyber-AI literacy, build knowledge and skills, and then take this knowledge home to their families, friends, and neighborhoods. In this way, we can enhance the circle of learning both directly (the students) and indirectly (helping around the home and with friends) within our communities. We must focus like a laser on supporting U.S. tech vulnerable populations,including younger people, the elderly, those lacking tech awareness, and historically marginalized populations. In this way, we can further expand societal awareness and preparedness for Cyber-AI and reduce/mitigate vulnerabilities and risks found within the digital environment.

One important role of higher education is to deliver relevant education and training programs for workforce preparation as well as enhance our organizational and personal resiliency by way of enhanced utilization of emerging technologies. As we all know, society is only as safe as the weakest link, and we must take proactive steps to enhance U.S. Cyber-AI literacy, skillsets, tools and techniques, and fundamental competencies for all residents through K-12 and Higher Education institutions and infrastructure.

### AI and Cybersecurity Impacting U.S. Higher Education in Remarkable Ways

AI is changing national higher education trends and practices in varied and impactful ways. Advancing Cyber-AI education, instruction, ethics, and community collaboration are prominent issues as tech evolves and transforms many aspects of society, including higher education, workforce development, governance, and campus technology services. Discussions of AI utilization, deployment, reasonable use, etc. are ongoing at all levels of education, type of institution, size of college/university, rural and urban, geographical location, or relative amount of funding. The impact of AI is found from top to bottom on the organizational chart at public and private colleges and universities. AI and security impact all academic units and departments as AI is both interdisciplinary and multidisciplinary. As AI implications are transformative, it is literally changing higher education, core university function and operations, administration, academics, and research overnight.

### Cyber-AI Convergence Impacting Higher Education Systems

This report section lays out a variety of ways that Cyber-AI technological convergence is impacting the organizational structure, mission, and operations of higher education and the academic community. In terms of higher education, AI is a growing priority on campus and is now commonly found on the agenda at the apex of the higher education system itself. In addition, Cyber-AI is impacting individual colleges and universities, academic units (like colleges and academic departments), faculty teaching, research, and service. Cyber-AI is also changing the student experience and redefining many programs, courses, and curriculum.

# Section 2- Advancing AI-Cybersecurity Convergence in Higher Education Curriculum, Pedagogy, Research, and Service

First, we discuss the impact of Cyber-AI on Higher Education Systems. The National Association of Higher Education (NASH) defines a public higher education system as a group of two or more colleges or universities, each having substantial autonomy and headed by a chief executive or operating officer, all under a single governing board and served by a system chief executive officer. [17] "We believe that systems can be coordinated players that leverage their power to convene and facilitate, along with their governing and policy-making authority, to build collaborations to support students and campuses, rather than trying to mediate competitive actions." [18] Examples of public higher education systems include the California State University (CSU) with 22 campuses and seven off-campus centers which together enroll 461,612 students and employ 63,375 faculty and staff members [19] , and the University of Arkansas System (UA System) with 7 universities, 8 community colleges, and 6 other units enrolling over 70,000 students and employing over 28,000. [20] There are many states with higher education systems serving a large number of specific campuses (and academic units) at the community college and/or university level. These Systems are critical in promulgating and advancing Cyber-AI education and workforce preparation as we discuss in further details.

Higher Education Systems includes faculty, students, and staff. Many of these systems need to strategically govern, invest in, governing, and deploying AI systems across their campuses and often with significant global online programs delivery capabilities. Higher education systems develop and academic policy, centralize administrative function, and approve the development of new degrees and academic programs on their respective campuses.

Currently, many state university systems seek to promulgate policies and acceptable use of tech and AI and responsible for providing technology services guidance to campus information security offices. Examples of proactive and innovative higher education system interactions with leading Cyber-AI industry and providers can be found in the collaborations and partnerships with the CSU and the California Community Colleges. Partnerships between the nation's largest public higher education system (CSU) and largest community college system (with over 2.1 million students) are excellent ways to reach out to large numbers of students. It is through commitments of resources, funding, and training that Cyber-AI can be quickly and effectively rolled out at the higher education system level.

### Cyber-AI Convergence at Higher Education Institutions

In addition to discussing higher education system-level activity in Cyber-AI, we also discuss the ways in which individual institutions are impacted across their campus ecosystems. In 2025, all sized higher education institutions are being significantly affected by Cyber-AI issues from the smallest college to the largest universities. Administration, technology services, academics,

[17] nash.edu/about-nash/ Accessed electronically on 9/20/2025.

[18] nash.edu/about-nash/ Accessed electronically on 9/20/2025.

[19] calstate.edu accessed electronically on 11/11/2025.

[20] Uasys.edu/about/  accessed electronically on 11/11/2025.

# Section 2- Advancing AI-Cybersecurity Convergence in Higher Education Curriculum, Pedagogy, Research, and Service

academic units (like the Colleges and Deans), departments, faculty, staff, and students are all impacted by technology convergences. AI and data analytics, machine learning, cybersecurity, and information security programs, degrees and certificates, courses, curriculum. Cyber-AI technological convergence issues are growing significantly and impacting more students, staff, and faculty across the U.S.

What is valuable to know is that all types of institutions are looking into AI and how it can be used effectively, ethically, and responsibly on their respective campuses. Some campuses are advanced adopters of Cyber-AI and conceptualizing and investing big money into the necessary systems to conduct AI enhanced and autonomous business, teaching, research, and community service operations and functionality. Deployment of Cyber-AI systems, models, and tools can be an expensive proposition for many colleges and universities. The financial impact of AI-ML-LLM deployment is a concern as campus funds are always tight and must come from another budget line to pay for. We need to make sure that funding mechanisms are in place, so large gaps do not emerge between campuses on the basis of affording (or not) key and cutting-edge technologies.

**Colleges and Departments-** Cyber-AI convergence is impacting all academic disciplines on a college and university campus. In the Higher Education sector, Colleges and Departments are key academic and organizational units on campuses. Colleges are typically organized with linked academic disciplines and range from the sciences, engineering, arts and humanities, social and behavioral sciences, health, agriculture and many other specific specializations. Within Colleges are nestled academic departments broken into various disciplines and supporting numerous professional fields and occupations. Some disciplines have embraced tech, AI, and Cyber quicker than others. It is important to note that many different academic disciplines and professional fields across campuses are forming the vanguard of Cyber-AI deployment and utilization. Furthermore, faculty perspectives within colleges and departments are also highly varied. While consensus may exist, that AI has the potential to significantly transform higher education, consensus quickly declines when discussing the specifics and details of how, what, and why.

Substantial potential and benefits for AI and Cyber learning exists within all colleges and academic disciplines in higher education. The diffusion of Cyber-AI technology is moving past just the “quick adopters” and techies and rapidly moving into the mainstream of scholarship and academia. It is safe to say that colleges and academic departments (i.e. academic units) have different views on the utilization of AI and academic engagement. Cyber-AI convergence is moving at differential speeds across the country. Furthermore, there are clearly a variety of strongly held faculty attitudes that either support or are suspicious of AI and AI culture. Some faculty view Cyber-AI as transformative to the human experience while others fear this technology is more disruptive to the general society and to a learning community on campus. In a recent poll, about 35-40% of the country signaled distrust and unhappiness with the growing utilization of AI.

### Cyber-AI Convergence Impacts for Higher Education Faculty

**Faculty-** Some faculty are very excited about using AI within their classrooms and cannot wait for the release of new models, tools, and techniques. Other faculty are reluctant to welcome AI into their classrooms. Some faculty feel powerless to stop AI's advance into higher education broadly speaking. And there is everything in-between both polar opposites.

Verbiage related to AI usage in academic policy manuals and classes are commonly found on contemporary college course syllabi these days. Sometimes AI usage is supported and encouraged in class. Other times, AI is discouraged or explicitly prohibited. Many higher education faculty are concerned about AI when used to write student assignments or assist with taking exams (or coding projects). Faculty may consider AI generated work as plagiarism or a violation of the campus honor or integrity codes. In 2025, there are computer science and computer engineering courses with all exams and written work completed in a classroom and instructors watching students to keep them from accessing smartphones (and other devices) while writing exams or in-class writing assignments. This trend appears to be growing within higher education these days, particularly in more technical departments and fields of study.

Academic and curriculum issues are under discussion and consideration at all colleges and universities today. There are many core issues found at the heart of the campus faculty governance structure, academic freedoms, and moving into areas like academic policy, resource dedication, branding, marketing, HR, and strategic communications. A struggle for consensus on acceptable/reasonable use of AI is ongoing today on many campuses. AI related academic issues are becoming more frequent today and many admin, faculty and students are not necessarily on the same page related to acceptable use (and other) related policies on campus. There are relatively few guardrails and legislation, policy, or even best-known practices for wide-spread campus utilization. This guidance and direction would be deeply appreciated by all higher education key partners and major stakeholders. Additional guidance and direction in this policy area would be a welcome development in higher education.

When talking about common faculty academic duties, they tend to fall into the following categories: teaching, research, and service. Cyber-AI can have a meaningful impact on all these roles.

**Teaching-** many faculty have a variety of teaching duties. Faculty have a somewhat variable teaching load within the classroom. Community colleges tend to have higher teaching loads and

# Section 2- Advancing AI-Cybersecurity Convergence in Higher Education Curriculum, Pedagogy, Research, and Service

research universities tend to each fewer courses each term. Faculty, instructors, and lecturers enjoy a good deal of academic freedom in general, and even more so when drawn within their specific academic disciplines and expertise. Faculty can be tenure track (Assistant Professors) or tenured senior faculty (Associate and Full Professors). Faculty can be full time instructors or part- time adjunct faculty. The technical aspects of AI and Cyber are often taught by those who work full time themselves within the greater industry and teach adjunct for a night class or two a week.

The role of faculty has evolved significantly with several teaching modalities found today on a college campus— face to face, hybrid, and online courses. Remote teaching and classes are widely available in post- COVID higher education. Faculty are found in many different disciplines these days in all teaching modalities—many teaching in several different delivery systems in a given semester. Given the role of technology in the "classroom" or the learning environment, all faculty are now impacted by AI and Cyber considerations. The convergence of Cyber-AI is directly impacting higher education faculty in their classrooms, learning spaces, communication modes, and general campus life. Not hard to find some type of AI event or symposium on a college or university campus these days.

**Research-** Another common feature of 4-year/6-year/doctoral granting institutions is found within the faculty research components of academia. These components include faculty writing grants, research resulting in publications, conference presentations, and related scholastic activities. Big data and AI are having a profound impact on campus and faculty research opportunities with AI playing a substantial interdisciplinary role in 2025.  The impact of AI is making a difference in how faculty and institutions conduct research and sustain related activities is impressive. We are seeing innovations here across the learning eco-system. In addition, many (if not all) academic units and disciplines are impacted by the transformative properties of AI. This trend and impact be transformative and sustained for years into the future of the AI era. One key point here is the value of data security while utilizing AI to conduct research. It is increasingly clear that AI systems, models, and data are being targeted malicious and need additional securing. This subject is discussed in further detail in Section 4- Campus Infrastructure and Security Practitioners further in this report.

**Service-** universities, faculty, staff, and students serve the university in a variety of ways, including committee-work, subcommittee work, mentoring and advising faculty and students. Faculty also serve the greater community in a variety of public facing (external ways) with their invaluable time and dedication. University and community service takes many ways and forms and more of these meetings and service involve the utilization of AI and also securing our respective cyberspaces. Service-based learning today is a common feature on many college and university campuses. With the flexibility offered by AI to conduct many forms of service and problem solving within our local communities, it is being used by faculty and students more frequently. AI can be directed at resolving stubborn social issues like homelessness or downtown city planning and efficient land use and then put into action by student-led teams. Given new opportunities with the utilization of AI models and systems to develop meaningful solutions to community problem, we should further enhance the use of AI faculty expertise in AI utilization in our service function at colleges and universities. In this way, as Cyber-AI impacts our institutions and communities as faculty and students lend their expertise to others to assist in diffusing and promulgating critical and complex emerging technologies through our campus function and responsibility to service.

There are many implications from higher education systems, campuses, colleges, academic departments, faculty, staff, and students. All groups are being highly impacted through the transformation found at the core of the convergence of Cyber-AI on a college and university campus. What is of critical importance is the development of a comprehensive national strategy for the growing issue of converged AI-Cybersecurity education and workforce preparation . Therefore, we describe the value of a career education pipeline and pathway to resolve these core and rising issues. Cyber-AI converged pipelines and pathways are essential to providing professional preparation for the next generation of specialized workforce as well as providing these new digital skills that are frankly essential "soft-skills" critical for all global citizens in the age of AI.

### The Value of Cyber-AI Education Pipelines and Pathways

We have discussed the importance of AI & Cyber education and training as a national priority and capability. With the size of the U.S. education and higher education sector, approximately 20% of the population, we can quickly transform society to keep up with game-changer Cyber-AI technology convergence rolling out globally. These future issues bring up important strategic questions of managing the role of Cyber-AI in Higher Education in the next few years. Many factors must be carefully considered as the foundations by which AI and Cyber are built, taught, and learned in K-12 and Higher Education. Pandora's box has been opened here. Cyber-AI issues and pressing policy issues are not going away anytime soon. Cyber-AI skills, tools, and preparation will be critical to the success of future generations of Americans.

Because of the deep transformative changes emanating across society due to AI; the critical need to secure our systems, networks, data and privacy, the K-12/Higher Education community should be the driving source of educating, preparing, and evolving societal trend towards Cyber-AI utilization and acceptable use of AI now and into the future. There is tremendous value in the digital environment to have wide access to a large cadre of specialized, prepared, and experienced AI and cybersecurity professionals and citizens. Wide access to a skilled workforce and zero issues with talent acquisition and retention should be an important national priority, capability, and worked towards diligently. AI Literacy and fluency are also important skills for everyone that utilizes technology.

The creation of an efficient and feasible Cyber-AI pipeline and pathway should be a key national strategic priority. Strategy and resource allocation to support Cyber-AI education, workforce development, and awareness/preparedness are particularly valuable today given current global security, economic competition, and the specter of geopolitical conflict. The present high threat conflict raises the currency and need for qualified and skilled information security and AI professionals. We do not want to fall behind our global adversaries on AI and cybersecurity matters. This is an "all hands-on deck" type of problem. The U.S. must find collaborative solutions with the advice, support, and technical assistance from all key partners and major stakeholders in the higher education sector. Public sector, private sector, NGOs, and academia must work together on this issue so we can all mutually benefit from these transformative and coordinated strategic efforts; and the critical policy and legislative initiatives to make them happen in a timely and proactive way.

The value of a fully functional Cyber-AI security pipeline and pathway (across all levels of education from pre-K to Ph.D. programs) available nationally to all interested citizenry, employees, and learners would position the U.S. long-term in a very favorable position moving forward into the AI era. We define and discuss two key concepts here for K-12 and Higher Education- pipelines and pathways. These are both very valuable approaches to Cyber-AI education and workforce development in the current and growing future digital world. These questions are further discussed in the next few report pages.

**Cyber-AI Pipelines-** A big picture approach to education and workforce development preparation aligned at all levels of education needed for various work roles. Pipelines run from PreK to Ph.D.'s, into the transition processto hiring, and then the working world for all steps of the career ladder from entry to executive level (and everything in between). Career education pipelines refer to aligned and carefully linked education programs across all levels of learning that start from very young children (to help build academic resiliency, fundamental knowledge, and positive peer interactions) to advanced graduate degree programs where future teachers, leaders, researchers, and other key specialized work roles are developed. Pipelines include a blend of additional career preparation components, including professional industry-based certifications, work experience (like internships, registered apprenticeships, Co-Op Programs, and Fellowships, etc.), professional socialization, mentoring, cyber competitions, boot camps, etc.

# Section 2- Advancing AI-Cybersecurity Convergence in Higher Education Curriculum, Pedagogy, Research, and Service

**Cyber-AI Pathways-** There are 52 current cybersecurity work roles found in the NICE Cybersecurity Workforce Framework v.2.0. [21] Each work role has its own related details, task statements, knowledge and skill statements, etc. In the NICE CWF alone, there are approximately 1007 task, 630 knowledge, 374 skill and 176 ability statements. [22] AI will add additional tasks, knowledge, skills, and abilities. This is a lot of curriculum and instruction to provide. Colleges and universities are very unlikely to have the resources, interest, and faculty expertise needed to teach everything at any one specific institution. Thus, we need to have multi campus consortiums collaborating across higher education (and closely linked with pK-12th and adult education programs) at the local, regional, statewide, and national levels. We should focus on designing pathways to keenly support various "high demand/hard to fill" jobs in key emerging/applied occupational clusters like in IT-Cyber-AI- Networking, and Quantum Computing.

### The Role of Higher Education in Cyber-AI Education, Literacy, Awareness, Preparedness, and Training

In fact, AI and cyber literacy and knowledge have now been elevated to "soft skills" or "essential skills" found within all employers including government, industry, and academic workplaces. Cyber-AI skills are growing in importance as they impact us increasingly daily. Given the importance of AI and Cyber literacy, awareness, and preparedness for everyone in a tech driven society, we must utilize K-12 and Higher Education to support and distribute knowledge and information to effectively utilize and secure their data, computers, networks, and privacy. Cybersecurity education took a tremendous step forward with the development of National Centers for Academic Excellence (N-CAE-C) and the release of the NIST NICE Cybersecurity Workforce Framework 1.0/2.0. However, it is critical that both advance further into the converged Cyber-AI skill sets and competencies of the future workforce.the workforce in terms of critical Knowledge, Skills, and Abilities (KSAs) and competencies. These impacts are being felt in all types of higher education institutions both public and private. It is important that the academic community enhances our Cyber-AI Pedagogy- and how these core skills are taught and learned by faculty and students. Cyber-AI is impacting programs, courses, curriculum, at the following levels of education. Many colleges and universities are in the process of adding new degree and certificate programs and courses on campus; and more faculty are utilizing AI within their curriculum and enhancing content and instructional materials.

2- Year Degrees/Certificates
4- Year Degrees/Certificates
6-Year (Graduate) Degrees and Certificates
Ph.D. Programs- (AI/Cyber/Data/Research Scientists)

[21] niccs.cisa.gov/tools/nice-framework/work-role. Accessed electronically on 10/12/2025.

[22] niccs.cisa.gov/tools/nice-framework/work-role. Accessed electronically on 10/12/2025.

# Section 2- Advancing AI-Cybersecurity Convergence in Higher Education Curriculum, Pedagogy, Research, and Service

### Directions for Future Cyber-AI Higher Education Activity

There are many questions about the impact of Cyber-AI convergence on higher education as we move into the transformative AI era. Work roles, KSAs, and tasks are changing substantially as machines do more work and tasks in digital security and other sectors across the U.S. As such, the way we prepare newer generations must change substantially as well.

- Critical Analysis of the current state of Cyber-AI Education Program and Courses? Who has programs and what do they look like? What kinds of AI-ML-Data-Cyber courses are typically taught at these institutions?

- Professional/Academic Certificate Program Capability Gap Analysis- Existing AI certificates (beginner, intermediate, advanced, executive AI Certifications).

- What types of workforce development and experiential learning opportunities are available today?

**Solution:** Design, develop, and implement an educational framework to include both a traditional "academic" and non-traditional "CTE/skills based" approach to include education programs (at all levels of education), stackable certificates linked from one level (foundational, beginner, intermediate, and advanced levels) to the next.

### Cyber-AI Soft-Skill Professional Preparation

It is becoming increasingly clear of a need to emphasize broader Cyber-AI skill sets across all work roles and as members of a modern and technological society. AI Literacy (preparedness and awareness) at all levels of K-12 and Higher Education is part of this transformative change. The best advice is to start children early and enhance their understanding, knowledge, and skills throughout the education cycle.

(AI Literacy and Culture). Development of AI Literacy programs (i.e. AI-Hygiene) across all generations and all ages is critical. Philosophical discussion of the use of AI and its guardrails are helpful, but we must strive towards further understanding of application and real-world experience. How can we improve our understanding of AI acceptable use, various limitations/its usage, and how to discern accurate AI versus data hallucinations or confabulation? Confabulation is when AI sounds like an authoritative source, but the information is otherwise made-up and no working links to the reference can be found. To emphasize AI in education, we need to start early and focus on imparting common sense and discretion as to how AI and security are concerned and intertwined.

# Section 2- Advancing AI-Cybersecurity Convergence in Higher Education Curriculum, Pedagogy, Research, and Service

The following section includes key Cyber-AI higher education recommendations. All courses need an AI module up front to assist students understanding the utilization and limitations of AI. We cannot always trust AI at face value, must always review model/prompt output, and need to be better consumers of AI systems, tools, models and  better protect valuable data.

## Broader Issues of Cyber-AI Convergence in Higher Education

All higher education institutions, including private and for-profit universities are under pressure to deploy, operate, and train AI systems, models, and tools in support of their institutions, students, faculty, and staff. AI is impacting key partners and major stakeholders, both directly and indirectly, in numerous ways as described in this section. A culture of AI and security is forming and evolving for both private and public institutions. This trend is consistent with the general utilization of the greater society and where future skills and jobs will be found. We must work with both public and private institutions of higher learning to deepen a culture of AI and security across U.S. schools, districts, colleges, and universities.

Many AI and security implications are found on college and university campuses today. Higher education campuses of all sizes are working on the discussion undergirding the relationship with transformative AI in such areas as reasonable/acceptable use cases, other industry best practices, as well as in policy and governance. How do we balance the needs of the many stakeholders and key partners our campus communities? Many campuses today have AI Task Forces, academic community committees, and analysts looking into how to best roll out products, services, and tools to our faculty, staff, and students. This conversation has had various levels of success on campuses.

There is a growing discussion (and debate) on how AI reasonable use is found in an academic setting in terms of education, teaching, research, and service. For example, there is a spirited discussion today of how students are using AI in class or for assignments turned in for credit and the academic policies and syllabi verbiage that govern these types of issues. Faculty, campuses, and students fall across a wide spectrum in terms of the utilization of AI in class assignments, academic research, research, and "homework." Student evaluation and assessment policies are moving through the faculty governance and academic policy processes as this is a pressing issue that needs some resolution and clarity on this aspect of campus life.

In all fairness, not all faculty are big fans of AI and what is happening as future AI continues to directly and indirectly impact higher education. Some question AI, think it is over-rated, cite the potential for disruption, economics, taking jobs away, and generally encroaching into human-centric sovereignty. By and large, it seems that the majority of faculty think positively about AI and are thinking of how to best integrate it within their teaching philosophy and by extension into the classroom. **But as this convergence continues, it will be interesting to see if these issues for institutions and faculty are resolved via consensus or through conflict.**

With vital roles AI is beginning to play in global society, it is critical to educate, train, and prepare out citizenry at all levels of education. We must promulgate emerging technologies education and training to all to fully utilize Cyber-AI safely and securely. How should this objective be accomplished? Through the creation and implementation of Cyber-AI Education Pipelines and Pathways at all levels of education from pre-Kindergarten through Ph.D. programs; that transition into the hiring process; and then all rungs of the career ladder from entry to executive level. This and other Cyber-AI convergence higher education recommendations are found below. These recommendations link and align with the following Report Section Three on workforce development and the creation of a new converged Cyber-AI work role discussed shortly.

### Advancing Cyber-AI in Higher Education Recommendations

1. **Higher Education System and Institutional Level Support-** provide SME and technical guidance on strategic Cyber-AI policy direction and guidance, maturity model framework development. Design, develop and implement a National Center of Cyber-AI Education, Research, and Teaching as well as regional hubs to promulgate best practices in Cyber-AI implement, and promulgate best practices related to higher education and the implications of converging emerging technologies such as AI, ML, Cyber, Quantum, and coordinate additional future innovative technologies as they arrive.

2. **Conduct Cyber-AI Workforce Development Education and Training Capability Gap Analysis and Labor Market Supply/Demand Study.** It is crucial to deepen our understanding of the key trends in Cyber-AI academia and what is occurring on colleges and universities in this Cyber-AI evolution. What colleges and universities have outstanding emerging technology programs? What are key aspects of these programs? How deep and efficient is the pipeline/pathway from K-12 and Higher Education and how do programs align and transition from one to the next? Once we understand what current higher education can deliver, we can identify the KSAs and gaps in the Cyber-AI workforce preparation process.

3. **We must develop an aligned, linked, comprehensive pathway for converged Cyber-AI Education and Workforce Development for professional career preparation-** Pathways that reflect both Cyber-AI domains should be available nationwide, accessible to urban and rural residents, and a critical step towards filling significant emerging capability gaps within the U.S. workforce. We need more cyber defenders within our workforce that are very well versed in AI skills and tools.

# Section 2- Advancing AI-Cybersecurity Convergence in Higher Education Curriculum, Pedagogy, Research, and Service

Cyber-AI Professional/Career Preparation Pathway
Traditional- “Academics”- STEM/STEAM-
Non-Tradition Model “Skills/Competencies”- CTE-

4. **Cyber-AI Soft Skills Education Development-** We must treat Cyber-AI skills and competencies as key soft skills needed by everyone across a modern technological society. Develop technical, non-technical, management, and executive-level educational pathways for Cyber-AI professional skill preparation as well as these soft skill sets necessary for success in today’s tech heavy world. Cyber-AI Literacy is as important a skill as digital and information literacy. Cyber-AI awareness and preparedness skills are as well and must be baked into the digital culture for 2025 and beyond.

5. **Implement Cyber-AI Education, Teaching, Research and Service Grant Programs-** Assist in the design, development and implementation of comprehensive and aligned Cyber-AI education programs including courses, curriculum, and applied projects in higher education institutions, classrooms, and labs. Given about 20% of the population is a student in K-12 and Higher Education, it is important to have funding mechanisms available to support a variety of new and innovative approaches to Cyber-AI teaching, learning, research, and service. Support should focus on interdisciplinary approaches, innovations found in diverse academic disciplines, and also integrate campus technology services offices into these academic initiatives.

Due to rapid speed of technological breakthroughs, it is vital to support new and innovative academic activity and classroom approaches through viable external grant funding support and project technical assistance.

[21] https://www.weforum.org/publications/the-future-of-jobs-report-2025/in-full/3-skills-outlook/ Accessed electronically on 10/20/25.

[22] https://www.axios.com/2025/08/26/ai-entry-level-jobs Accessed electronically on 10/20/25.

[23] https://www.cnbc.com/2025/09/07/ai-entry-level-jobs-hiring-careers.html Accessed electronically on 10/20/25.

[24] https://digitaleconomy.stanford.edu/publications/canaries-in-the-coal-mine/ Accessed electronically on 10/20/25.

# Section 3- Advancing Cyber-AI Workforce Development Convergence

## Section Lead- Dr. Keith Clement, Professor, Fresno State University, ATARC Cybersecurity Education and Workforce Development Academic Chair

### Introduction

How is the convergence of AI and cybersecurity impacting U.S. education and workforce development? We are interested in analyzing these implications from a variety of SME perspectives. Report Sections One and Two discussed the advancement and impacts of the AI-Cyber convergence trend found within broader society but primarily focused on K-12 and Higher Education. How we prepare current and future Cyber-AI professionals is of vital importance to future national and economic security. The same can be said about the importance of preparing our citizenry with these critical skill-sets to support societal and individual preparedness, awareness, and literacy into the AI age. The World Economic Forum (WEF) expects 170 million new jobs created by AI. [23] This is an important national priority and strategy that we should embrace through the smooth operation of a seamless Cyber-AI pipeline and pathway at all levels of the education process, that includes blended industry recognized professional certifications, tools and techniques, and work experience. The Cyber-AI pipeline and pathway is described briefly in the previous report section.

On many levels, entry level roles are declining in a competitive job market as industry and employers retool for the AI era and digital skillsets. Stanford Researchers report a 13% decline in employment for early career workers (ages 22-25) in the most "AI-exposed" occupations since the adoption of generative AI. [24] The convergence of Cyber-AI has (and will continue) to change the necessary job skill sets that employers and industry (public and private) are seeking into the future. It is also having a significant impact on the career ladder as well. Postings for entry-level jobs in the U.S. have declined about 35% since January 2023…with AI playing a big role. [25] Sectors like customer service, software development, and data entry are seeing steep declines due to automation. [26] In career clusters with large numbers of "machine tasks" found on the job, there is a good chance that AI is doing more of those types of those tasks, like in software development and coding, for example.

As such, industry specialized domain professional preparation process has (and will continue) to evolve significantly, particularly as agentic and automation in AI continues to grow and foster additional change within the cybersecurity eco-system. As a result, employers are seeking those with heavy Cyber-AI skills and avoiding those with fewer such skills, fluency, and acumen.

The WEF *Future of the Jobs Report* indicates that employers expect 39% of workers' core skills to change by 2030. [27] WEF cites "skill evolution" in technological skills growing in importance quicker than other types of skills and from 2025 to 2030 include AI and big data, networks and cybersecurity, technological literacy, creative thinking, resilience/flexibility/agility, and curiosity/

[23] https://www.weforum.org/publications/the-future-of-jobs-report-2025/in-full/3-skills-outlook/ Accessed electronically on 10/20/25.

[24] https://www.axios.com/2025/08/26/ai-entry-level-jobs Accessed electronically on 10/20/25.

[25] https://www.cnbc.com/2025/09/07/ai-entry-level-jobs-hiring-careers.html Accessed electronically on 10/20/25.

[26] https://digitaleconomy.stanford.edu/publications/canaries-in-the-coal-mine/ Accessed electronically on 10/20/25.

[27] https://www.weforum.org/publications/the-future-of-jobs-report-2025/in-full/3-skills-outlook/ Accessed electronically on 10/20/25.

lifelong learning. [28] WEF reports that 60% of workers will need new training. [29] Future workforce must reskill or risk getting replaced at work, either by AI or by better skilled workers. These are pretty dramatic choices to be considered by potential future workers.

Evolving future workforce trends favor those with strong technological and soft-skill sets. By 203, what are today considered workforce development critical skills today are projected to become even more important. [30] AI-Cybersecurity workforce skills will elevate from "optional" to core skills of the near distant future. At some point, everyone employed in a modern and tech heavy workforce will need digital soft-skills to get hired and maintain employment. Employers also expect strong soft-skills to include superior oral and written communications, team-based attitude, collaborative nature, and ability to show up to work on time, etc. Organizational workers will need utilize AI to assist them in completing their daily future work assignments quicker than if they did all the work themselves (e.g. without the assistance of AI).

So, the workforce preparation process will continue to evolve as the Cyber-AI transformation continues. In addition, the nature of future work roles themselves will continue to change and evolve as the necessary tasks and KSAs to secure and maintain those jobs changes over time as well. Cyber-AI professional skills and competencies are greatly needed currently and more so into the future. Cyber-AI skillsets are considered important across many sectors, occupations, and employers across the country and this value only continues to grow as AI becomes more impactful of the day to day working world.

One key problem from a workforce development perspective is the sheer pace of innovation in emerging tech (like AI, Cyber, ML, etc.) is much quicker than K-12, Colleges, and Universities can keep pace with. Tech innovations are announced near daily, but it takes years for many colleges and universities to develop and implement degree programs and courses due to barriers like the campus curriculum approval process. Quickly changing Cyber-AI skillsets and competencies translates into creation of new academic programs (degrees and certificates), relevant courses that teach key tools and techniques, cutting edge curriculum, pedagogy, research, workforce opportunities, etc. means that relevant education and training will increase in value in the future. However, the delay from innovation in tech to relevant programs and courses remains elusive at the national and state levels.

The struggle to keep up is real and exacerbated by continual funding and resources limitations found in K-12 and Higher Education. The business model is changing, the workplace is changing, and the classroom is changing. The implications of Cyber-AI convergence in workforce development are profound and the future labor pool and requisite skills, competencies, and career preparation processes are going to look remarkably different very soon.

[28] https://www.weforum.org/publications/the-future-of-jobs-report-2025/in-full/3-skills-outlook/ Accessed electronically on 10/20/25.

[29] https://www.weforum.org/publications/the-future-of-jobs-report-2025/in-full/3-skills-outlook/ Accessed electronically on 10/20/25.

[30] https://www.weforum.org/publications/the-future-of-jobs-report-2025/in-full/3-skills-outlook/ Accessed electronically on 10/20/25.

# Section 3- Advancing Cyber-AI Workforce Development Convergence

### Implications of Cyber-AI Convergence in U.S. Workforce Development

AI is having a tremendous impact on cybersecurity education and workforce development in transformative ways for both red team (attack) and blue team (defensive) activities. In this report section, we analyze and evaluate the intersection between converging Cyber-AI professional workforce development for employers and the education preparation process for candidates in schools, colleges, and universities nationwide. We need to understand what industry and employers (both public and private sector) are looking for in terms of hiring and talent acquisition to best prepare future workforce. Key sources of Cyber-AI standards include NICE Cybersecurity Workforce Framework (2.0), NICE AI RMF work roles and applicable task statements and KSAs sought in prospective new hires and found in the previous report section. In Section Three, discuss the preparation process and propose a workforce-oriented curriculum architecture by which future Cyber-AI job candidates will be readied for employment in this rapidly changing professional field in a series of tables and charts found on the next few pages.

The proposed Cyber-AI professional framework lays out key components to address in current skills gaps for both AI and cybersecurity workforce developing because of the tech convergence process. How to develop a preparation framework by which employer minimum/preferred job requirements can be met with Cyber-AI education programs, industry based professional certifications, and on the job training (workforce) opportunities? Through the development of a converged Cyber-AI professional work role that meets the needs and requirements for each specific domain. These issues are discussed in further detail after we discuss key Cyber-AI workforce preparation components and modes.

GRAPHIC #3: AI-Cybersecurity Workforce Preparation Components

Cyber-AI job preparation process includes the following components:

Education/training programs-

Industry based professional certifications-

Work experience- On the Job Training (OJT)-

Networking and Professional Socialization (including mentoring)-

Transition into career & workplace- mentoring and advising

GRAPHIC #4: Modes of AI-Cybersecurity Workforce Development:

Internships- (paid/unpaid)-

Pre Apprenticeship programs-

Registered Apprenticeships-

Co-ops- an engineering approach to workforce development-

Fellowships-

Volunteer experiences-

# Section 3- Advancing Cyber-AI Workforce Development Convergence

### Recommendations to Enhance AI-Cybersecurity Infused Workforce and Career Development

Linkages to both the traditional and non-traditional approaches to Cyber-AI security education and workforce preparation  are critical. This report seeks to provide recommendations on workforce and career preparation measures to meet future Cyber-AI converged workforce needs for both college-prepared and Career Technical Education (CTE) pathways of professional development. Towards that objective, in the following section we introduce a proposed new converged Cyber-AI work role that spans all levels of the career ladder from entry- level, intermediate, advanced and executive level positions. These rungs of the career ladder are blended, linked, aligned and transition seamlessly from one level of the career ladder through the next. In this way, we can develop replicable programs and courses that could be utilized by higher education institutions and the workforce/labor training providers nationwide.

### Introduction to a Proposed Converged Cyber-AI Workforce Development Work Roles and Aligned Stacking Curriculum Reference Architecture Framework

From the previous report pages, it has become increasingly clear that converged Cyber-AI is here and in the process of fully unfolding and evolving. This continued period of transformation and change is going to continue in the near (and perhaps long term). That does not mean that we “wait a few years” until the pace of tech innovation subsides a bit, certainly as far as AI and cybersecurity go. **Rather, we should start designing a converged Cyber-AI work role and proposed stacking curriculum framework now to accompany this “new” converged work role of the future.** This architecture is the first step to reference and guide educators and workforce professionals in the quickly growing field of Cyber-AI. As this is a completely new and innovative approach to workforce preparation for converged Cyber-AI professional roles in the future, this curriculum will evolve. We are building upon existing work roles to envision this new type of position and conceptualize on what is needed moving forward.

The next few pages contain a variety of tables and charts for upcoming Cyber-AI converged workforce roles, including modules, skills developed, and relevant framework alignment and mapping. In addition, we fill in topics, tools, and outcomes for these Cyber-AI converged work roles from entry level, intermediate, advanced, and executive level positions. The report authors propose there is a significant future need for converged Cyber-AI work roles to support this intersectionality.

To support these new work roles, we lay out an aligned stacking curriculum architecture that runs throughout the career ladder from entry-level, intermediate, advanced, and executive-level positions. Future Cyber-AI professionals are critical at all levels of the career ladder and the relevant preparation process must be linked and transition seamlessly from one work role level to the next. For each level of this curriculum architecture structure, we describe the target audience, strategic goals, and phases/modules of the Cyber-AI converged pipeline and pathway for utilization across U.S. Education and Workforce Development. Modules include key objectives, important topics, and cutting-edge tools. In addition, curriculum phases discuss specific modules, skills developed, and relevant framework alignments. At the entry, intermediate, advanced, and executive levels, we lay out key modules, focus areas, and suggested types of professional industry-based certificate and credential frameworks.

The entry, intermediate, and advanced levels share a variety of structural and organizational commonalities. These include:

Strategic Foundations
Technical Mastery
Application, Deployment, and Operations
Capstone, Certificates, and Credentials

The executive level typology is significantly different than the other work role levels of converged Cyber-AI professionals. This is due in part to the significant contextual and industry specific business processes and government practices and policies that may not be a primary focus of the other work roles. This variation is reflected in both the architecture structure and specialized curriculum found for the executive level of Cyber-AI leadership, decision-makers, and legislators.

Strategic Awareness and Risk Framing
Oversight and Investment Strategy
Governance, Ethics, and Compliance
Capstone, Certifications, and Credentialing

### Introduction to a Proposed Converged Cyber-AI Workforce Development Work Roles and Aligned Stacking Curriculum Reference Architecture Framework

#### Strategic Goals:

1. Develop Cyber-AI Hybrid Talent Model and Pipeline- equip professionals with technical, operational, and governance-level skills.

2. Align Model and Pipeline with National Frameworks- integrate model and pipeline with NIST NICE, AI RMF, ISO/IEC 42001, and DoDM 8140.03 standards.

3. Accelerate Credentialing & Career Mobility- design and offer stackable architecture for microcredentials, digital badges, and role-based pathways.

4. Foster and Enhance Public-Private-Academia Collaboration- engage with major partners and key stakeholders in co-designing curriculum and workforce development opportunities like registered apprenticeships and paid internships.

5. Promote Ethical AI Deployment and Operations- Embed fairness, transparency, equity, and accountability into all education and training programs.

### Phase 1: Foundations: (Weeks 1-4)

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

### Module 1: Cybersecurity Foundations

Objective: Build baseline security awareness and technical fluency

Topics:
CIA triad, threat types, encryption, IAM
Network protocols (TCP/IP, DNS, HTTP)
Linux command line and system hardening

Tools: Industry tools like Wireshark, Nmap, Kali Linux
Outcome: Prepare for industry-based certification like: CompTIA Security+ or ISC2 CC

### Module 2: Cloud Security for AI Workload

Objective: Understand how AI systems operate in cloud environments.

Topics:
IAM in AWS/Azure/GCP
Securing AI APIs and containers
Cloud-native monitoring and logging
Tools: Industry tools like Terraform, Kubernates (intro), CloudTrail
Outcome: Prepares for SC-900 or CSSP (Associate level)

# Section 3- Advancing Cyber-AI Workforce Development Convergence

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

| Module | Skills Developed | Framework Alignment |
|---|---|---|
| Intro to Machine Learning | Supervised/unsupervised learning, model evaluation | NIST AI RMF: Map & Measure |
| Adversarial ML & Model Risks | Evasion, poisoning, inversion attacks | NICE: SP-RSK-002, Risk Analyst |
| AI Ethics & Governance | Bias, fairness, NST AI RMF, ISO/IEC 42001 | NICE: OV-GOV-001, Governance Specialist |

### Module 3: AI Literacy for Security

Objective: Introduce AI concepts relevant to security contexts

Topics:
ML basics: classification, clustering, model evaluation
AI pipeline components: data, training, inference
Bias, fairness, and ethical considerations

Tools: Industry tools like Jupyter Notebooks, scikitllearn, TensorFlow
Outcome: Prepare for industry-based certification like: Foundation for IBM AI Engineering or BlueCert AI Security

### Module 4: Governance, Risk, and Compliance

Objective: Align AI systems with ethical and regulatory standards.

Topics:
NIST AI RMF: Map, Measure, Manage, Govern
ISO/IEC 42001, GDPR, and AI audit prep
Risk registers and policy documentation

Tools: Industry tools like RiskLens, compliance dashboards
Outcome: Supports roles in AI governance and compliance.

# Section 3- Advancing Cyber-AI Workforce Development Convergence

### Phase 3: Applied Security (Weeks 9-12)

| Module | Skills Developed | Framework Alignment |
|---|---|---|
| SIEMs & Threat Detection | Data analysis tools, ELK, anomaly detection | NICE: PR-INF-001, Incident Responder |
| Secure AI Deployment | Model monitoring, drift detection, API security | NIST AI RMF: Manage & Govern |
| Hands-on Labs & CTFs | Red/blue team exercises, adversarial ML simulations | NICE: PR-CDA-001, OM-ANA-001 |

### Module 5: Applied Security

Objective: Introduce AI concepts relevant to security contexts

Topics:
ML basics: classification, clustering, model evaluation
AI pipeline components: data, training, inference
Bias, fairness, and ethical considerations

Tools: Industry tools like Jupyter Notebooks, scikitllearn, TensorFlow
Outcome: Prepare for industry-based certification like: Foundation for IBM AI Engineering or BlueCert AI Security

### Phase 4: Certification, Credential, and Career Prep (Weeks 13-16)

| Module | Outcome |
|---|---|
| Certification Prep | e.g. Security+ or SC-900 or BlueCert AI Security Foundations |
| Portfolio Development | Documented labs, GitHub projects, AI threat models |
| Career Coaching | Resume, interview prep, job role mapping to NICE Framework |
| Cyber-AI Pathways | Functioning Cyber-AI education pathway program from K-12 Education through Ph.D.'s |

# Section 3- Advancing Cyber-AI Workforce Development Convergence

### Module 6: Capstone & Career Readiness

Objective: Apply skills in real-world scenarios and prepare for job entry.

Activities:
Red/blue team simulations with AI components
Portfolio development (GitHub, documentation)
Resume building, interview prep, NICE role mapping

Outcome: Job-ready candidate with mapped competencies and KSAs.

### Intermediate-Level Converged Cyber-AI Workforce Development Work Roles and Stacking Curriculum Framework

### Strategic Goals:

1. Develop Cyber-AI Hybrid Talent Model and Pipeline- equip professionals with technical, operational, and governance-level skills.

2. Align Model and Pipeline with National Frameworks- integrate model and pipeline with NIST NICE, AI RMF, ISO/IEC 42001, and DoDM 8140.03 standards.

3. Accelerate Credentialing & Career Mobility- design and offer stackable architecture for micro-credentials, digital badges, and role-based pathways.

4. Foster and Enhance Public-Private-Academia Collaboration- engage with major partners and key stakeholders in co-designing curriculum and workforce development opportunities like registered apprenticeships and paid internships.

5. Promote Ethical AI Deployment and Operations- Embed fairness, transparency, equity, and accountability into all education and training programs.

# Section 3- Advancing Cyber-AI Workforce Development Convergence

### Intermediate Cyber-AI Converged Program Curriculum Structure (12-16 Weeks)

| Phase | Focus Area | Credential Outcomes |
|---|---|---|
| 1. Strategic Foundations | AI threat landscape, governance, NIST AI RMF | ISC2 AI Strategy Certificate |
| 2. Technical Deep Dive | Adversarial ML, secure deployment, cloud security | CERT AI for Cybersecurity Certificate (SEI/CMU) |
| 3. Operational Integration | AI-enhanced threat intelligence, incident response | EC-Council Generative AI for Cybersecurity |
| 4. Capstone & Career Readiness | Project examples: Secure AI system design, audit simulation | Digital portfolio and projects |

### Phase 1: Strategic Foundations (Weeks 1-2)

| Module | Focus | Outcomes |
|---|---|---|
| AI-Cybersecurity Convergence | Strategic overview of AI's impact on threat landscapes and defense models | Understand AI-driven threats, automation in SOCs, and workforce implications |
| AI Risk Management and Governance | NIST AI RMF, ISO/IEC 42001, privacy impact assessments | Apply governance models to AI systems and assess compliance risks |

### Phase 2: Technical Deep Dive (Weeks 3-6)

| Module | Focus | Tools and Skills |
|---|---|---|
| Adversarial Machine Learning | Evasion, poisoning, model inversion, robustness testing | Industry tools like PyTorch, CleverHans, ART |
| Secure AI Development | API hardening, access control, model monitoring, drift detection | Industry tools like Kubernetes, MLflow, Vault |
| Cloud Security- AI Workloads | IAM, container security, cloud-native threat detection | Industry tools like AWS IAM, Azure Sentinel, Terraform, etc. |

# Section 3- Advancing Cyber-AI Workforce Development Convergence

### Phase 3: Operational Integration (Weeks 7-9)

| Module | Focus | Tools and Skills |
|---|---|---|
| AI-Augmented Threat Intelligence | Using LLM and ML tools for threat detection and analysis | Build AI-enhanced dashboards, simulate threat hunting |
| Incidence Response for AI Systems | Responding to model compromise, data leakage, inference manipulation | Tabletop exercises, forensic analysis labs |
| Ethical Oversight & Audit Readiness | Bias mitigation, fairness audits, stakeholder reporting | Draft audit reports, simulate ethical reviews |

### Phase 4: Capstone, Certificates, & Credentialing (Weeks 10-12)

| Component | Description |
|---|---|
| Capstone Project | Design & defend a secure AI system with governance documentation |
| Micro-Certification Stacking Architecture | Select 2-3 targeted credentials, like Adversarial ML Defense, AI Governance, Cloud Security for AI |
| Digital Portfolio & Career Mapping and Pathways | NICE work role alignment, resume refinement, interview coaching, mentoring, Cyber-AI career pipelines |

### Advanced-Level Converged Cyber-AI Workforce Development Work Roles and Stacking Curriculum Framework

### Strategic Goals:

1. Develop Advanced Cyber-AI Talent Model and Pipeline- train professionals in adversarial ML, LLM security, cloud-native AI protection, and AI governance.

2. Align Model and Pipeline with National Frameworks- integrate model and pipeline with NIST NICE, AI RMF, ISO/IEC 42001, and DoDM 8140.03 standards.

3. Accelerate Credentialing & Career Mobility- design and offer stackable architecture for micro-credentials, digital badges, and role-based pathways.

4. Foster and Enhance Public-Private-Academia Collaboration- engage with major partners and key stakeholders in co-designing curriculum and workforce development opportunities like registered apprenticeships and paid internships.

5. Promote Ethical AI Deployment and Operations- Embed fairness, transparency, equity, and accountability into all education and training programs.

### Advanced Cyber-AI Converged Program Curriculum Structure (16-20 Weeks)

#### Phase 1: Strategic Foundations (Weeks 1-2)

| Module | Focus | Outcomes |
|---|---|---|
| AI Threat Landscape & Strategic Risk | Mapping AI-enabled threats, LLM misuse, & autonomous agents | Develop threat models for AI systems |
| AI Governance & Secure-by-Design Principles | NIST AI RMF, ISO/IEC 42001, ethical oversight | Draft governance framework & audit plans |

#### Phase 2: Advancing Technical Mastery (Weeks 5-10)

| Module | Focus | Tools and Skills |
|---|---|---|
| Neural Networks and LLM Security | Fine-tuning, prompt injection, RAG, LangChain agents | Industry tools like LLamaIndex, Streamlit, HuggingFace Transformers |
| Adversarial ML Engineering | GANs, model inversion, evasion, poisoning | Industry tools like PyTorch, CleverHans, ART, custom attack simulations |
| Anomaly Detection & Reinforcement Learning | Adaptive security, behavioral modeling | Industry tools like RLib, OpenAI Gym, custom policy tuning |

# Section 3- Advancing Cyber-AI Workforce Development Convergence

### Phase 3: Secure AI Deployment and Operations (Weeks 11-14)

| Module | Focus | Tools and Skills |
|---|---|---|
| Cloud-Native AI Security | Securing AI in cloud service environment providers, container hardening | Industry tools like Terraform, Kubernetes, Vault, CloudTrail |
| AI-Augmented SOC Operations | LLMs in SIEM, automated triage, threat hunting | Data analysis tool, GBT integration, SIEMs, ELK |
| Zero Trust for AI Systems | Identify, access, and inference control | ZTA frameworks, API gateways, model access policies |

### Phase 4: Capstone, Certificates, & Credentialing (Weeks 15-20)

| Component | Skills Developed |
|---|---|
| Capstone Project | Design & defend a secure, governed AI system with adversarial testing. |
| Credential Stack | ISC2 Secure-by-Design AI, CERT AI for Cybersecurity, EC-Council GenAI Security |
| Digital Portfolio & Career Mapping & Pathways | NICE CWF 2.0 Work Role alignment, executive briefing prep, peer-reviewed showcase and highlights |

### Executive-Level Converged Cyber-AI Workforce Development Work Roles and Stacking Curriculum Framework

### Strategic Goals:

1. Equip Executives with Cyber-AI Oversight Skills- train leaders in AI risk framing, governance, and strategic response.

2. Align Model and Pipeline with National and Global Standards- integrate model and pipeline with NIST AI RMF, ISO/IEC 42001, DoDM 8140.03, and GDPR.

3. Accelerate Credentialing & Career Mobility- design and offer stackable architecture for executive-level certificates, micro-credentials, digital badges, and board-ready governance playbooks.

# Section 3- Advancing Cyber-AI Workforce Development Convergence

4. Foster and Enhance Public-Private-Academia Collaboration- engage with major partners and key stakeholders in co-designing leadership curriculum and workforce development and retention opportunities.

5. Promote Ethical AI Deployment- Embed fairness, transparency, equity, and accountability into executive decision-making.

### Executive Converged Cyber-AI Curriculum Structure (8-12 Weeks)

### Phase 1: Strategic Awareness & Risk Framing

| Module | Focus | Outcomes |
|---|---|---|
| AI-Cybersecurity Convergence | Understand how AI transforms threat landscapes and defense models | Identify strategic risks and opportunities across sectors |
| AI Risk and Governance Frameworks | NIST AI RMF, ISO/IEC 42001, GDPR, DoDM 8140.03 | Apply governance models to enterprise AI systems |

### Phase 2: Oversight & Investment Strategy

| Module | Focus | Tools and Skills |
|---|---|---|
| AI Threat Intelligence & LLM Risk | Deepfake, prompt injection, autonomous agents | Evaluate vendor risk and internal exposure to generative AI threats |
| Secure-by-Design AI Strategy | Procurement, deployment, and lifecycle security | Build oversight models for AI system acquisition & integration |
| Incident Response Leadership | AI-enabled breaches, forensic readiness and analysis | Lead cross-functional response teams and board-level communications |

# Section 3- Advancing Cyber-AI Workforce Development Convergence

### Phase 3: Governance, Ethics, and Compliance

| Module | Focus | Outcomes |
|---|---|---|
| AI Ethics & Accountability | Bias, fairness, equity, explainability, human in the loop | Establish ethical review boards and stakeholder engagement plans |
| Audit & Regulatory Readiness | Privacy impact assessments, compliance mapping | Prepare for AI audits and regulatory disclosures across jurisdictions |

### Phase 4: Capstone, Certificates, and Credentialing

| Component | Skills Developed |
|---|---|
| Capstone Simulation | Lead a simulated AI breach response and governance review |
| Credential Options | Duke AI & Cybersecurity for Leaders Certificate, ISC2 AI Strategy Certificate, ISACA AI Risk and Ethics |
| Executive Portfolio | Strategic pathways roadmaps, governance playbook, board briefing materials |

# Section 4- From Static Defenses to Self-Evolving Systems: The Security Practitioner's AI Imperative

Prepared by: Eric Wall, CISSP, CISM, Chief Information Security Officer (CISO) – University of Arkansas System, ATARC Cybersecurity Education and Workforce Development Working Group Academic Co-Vice Chair
Gregory W. Cooper, Head of Information Systems Operations Center (ISOC), New Mexico State University, ATARC Cybersecurity Education and Workforce Development Working Group Academic Co-Vice Chair

### Introduction

Artificial Intelligence is not coming, it has arrived, reshaping the cybersecurity battlefield in real time. Once confined to experimental labs or niche analytics use cases, AI now plays a pivotal role across every phase of the cyber kill chain. It builds malware, generates deepfakes, evades detection, automates reconnaissance, and adapts to countermeasures faster than any human team can respond.

For security practitioners, this isn't just a shift in tooling; it's a shift in tempo, terrain, and threat actor capability. This chapter is a guide through that shift. It is written not for theorists or futurists, but for CISOs, SOC analysts, red teamers, compliance officers, and AI engineers who sit at the intersection of operational defense and technological disruption.

We begin by exploring how adversaries weaponize AI from machine learning-powered malware to synthetic identities and model evasion tactics. But we also highlight the equally powerful role AI plays in defending systems: detecting threats in real time, automating response, surfacing anomalies buried in terabytes of logs, and enabling predictive intelligence at scale.

We then examine how AI is transforming red team and blue team operations – not as a replacement for human skill, but as a co-pilot that augments realism, deception, and decision-making. From AI-powered honeypots to live-training simulations, security operations are evolving into cyber wargames where both attackers and defenders are increasingly augmented by machine intelligence.

But with power comes responsibility. We dedicate an entire section of this chapter to the ethical, legal, and privacy concerns that surround security-focused AI because bias, misuse, and lack of transparency are not abstract risks. They are realities that can erode trust, violate regulations, and introduce new attack surfaces inside the tools meant to protect us.

# Section 4- From Static Defenses to Self-Evolving Systems: The Security Practitioner's AI Imperative

That's why we also explore how to secure the AI itself: protecting models from poisoning, securing cloud-based AI infrastructure, and continuously validating model behavior over time. The line between "AI used for security" and "security for AI" is becoming increasingly blurred and security leaders must be prepared for both.

Finally, we look ahead: at generative AI's growing role in future threats, the intersection of quantum computing and AI, and how to navigate the early to mid-stage adoption curve while preserving competitive advantage. In this next wave of transformation, success won't go to the teams with the flashiest tools, but to those who understand the delicate balance between automation, human oversight, and ethical guardrails.

## AI as an Adversary - Threat Landscape and Challenges

AI has emerged as one of the most potent force multipliers in the offensive arsenal of threat actors. While defenders have leveraged machine learning for years, adversaries are now catching up – and in some domains, surpassing us. From social engineering to malware automation, AI enables attackers to operate at greater scale, speed, and stealth than ever before. As security practitioners, it's critical to understand not only what these technologies can do, but how they're already being used against us in the wild.

### Machine Learning in Malware and Phishing

Traditionally, malware authors relied on obfuscation, polymorphism, and evasion tricks to bypass defenses. With AI, those capabilities are now fully automated and contextual. Language models can write phishing emails tailored to individual targets, often using scraped data from social media and public websites to adjust tone, language, and urgency. In some cases, phishing content is generated in real time during active conversation threads, creating believable interactions that are increasingly indistinguishable from human communication.

Meanwhile, malware development has begun incorporating reinforcement learning techniques that optimize payload behavior based on the target environment. Malware variants can assess sandbox behaviors, adapt network communication patterns, and avoid common triggers used by endpoint detection systems – all without human intervention.

### Adversarial AI: Evasion Through Manipulation

One of the more sophisticated offensive uses of AI lies in attacking the very ML models defenders rely on. Through adversarial examples, attackers introduce subtle, often imperceptible changes to inputs that cause misclassification. For instance, a malware file could be crafted to bypass a model-based antivirus engine by exploiting its learned weaknesses without changing the core malicious behavior.

Other tactics include data poisoning, where attackers inject corrupted data into the model's training pipeline, or model extraction, where an attacker probes a deployed model's API to reverse-engineer its logic. These attacks challenge the assumption that AI systems are inherently more secure simply because they are complex or opaque.

**Synthetic Identities and Deepfakes**

Deepfakes and synthetic identity generation have moved from novelty to operational capability. GANs (generative adversarial networks) and diffusion models can now produce high-resolution faces, voices, and even interactive avatars. These tools are being used to bypass KYC (Know Your Customer) processes, impersonate executives in BEC (Business Email Compromise) scams, and conduct espionage or misinformation campaigns.

Deepfake voicemails or video calls (once easy to spot) have become good enough to fool employees, vendors, and even security teams. Combined with social engineering and AI-enhanced pretexting, attackers can manipulate trust at scale.

**Automated Vulnerability Discovery**

AI models trained on codebases and configuration data can now identify potential vulnerabilities including complex chains that human pentesters might miss. Tools like GitHub Copilot (or similar open-source tools) are being repurposed to scan for known CVEs, hardcoded secrets, and privilege escalation paths. This capability collapses the timeline between vulnerability discovery and exploitation, forcing defenders to accelerate patching and response cycles.

Moreover, AI doesn't need to "understand" a vulnerability in the human sense, it simply needs to recognize patterns and exploit paths that historically led to compromise.

**AI-Driven Social Engineering**

Perhaps the most impactful application of AI in offensive operations is in social engineering. Generative models can now emulate tone, diction, cultural context, and emotional nuance. Attackers no longer need to be native speakers or skilled writers to produce highly believable phishing content, business correspondence, or customer support interactions.

Tools are also emerging that combine AI with behavioral psychology to optimize the timing, channel, and tone of outreach, effectively maximizing the likelihood of a response or action. These tactics target the softest parts of the security perimeter: users, service desks, and frontline staff who are under pressure and unaware of how far AI has evolved.

# Section 4- From Static Defenses to Self-Evolving Systems: The Security Practitioner's AI Imperative

## AI for Defense: Applications and Frameworks

While AI has rapidly evolved into a powerful weapon in the hands of adversaries, it is also becoming an indispensable ally for defenders. Security teams are using artificial intelligence not just to keep pace with attackers, but to fundamentally reshape how we detect, prioritize, and respond to threats. From large-scale anomaly detection to natural language understanding of unstructured threat intel, AI helps practitioners extend visibility, accelerate response times, and reduce cognitive overload in the SOC.

### Threat Detection and Anomaly Detection

AI excels at pattern recognition, and one of its most mature applications in cybersecurity is anomaly detection. Traditional rule-based detection systems are prone to gaps and false positives, especially in complex environments with large volumes of log data. AI models, especially unsupervised or semi-supervised ones, can identify deviations from normal behavior in real time, flagging threats that would otherwise go unnoticed.

For example, if a user begins accessing sensitive files outside of business hours from an unusual IP range, AI can flag the event without needing a static rule. When trained on historical behavior, these models can detect lateral movement, privilege escalation, or data exfiltration attempts, well before an attack reaches the point of damage.

More advanced implementations leverage ensemble models that combine endpoint telemetry, identity behavior, and network flow data to correlate signals across domains. These capabilities are now being embedded in platforms like Microsoft Sentinel, CrowdStrike Falcon, and Google Chronicle, enabling security operations centers to identify unknown unknowns with greater accuracy.

### Predictive Analytics for Threat Intelligence

AI-driven threat intelligence platforms are moving from reactive aggregation to proactive forecasting. By ingesting and analyzing structured and unstructured data including dark web chatter, attack indicators, and malware telemetry, AI models can help predict which threats are most likely to target an organization or sector.

Some models correlate threat actor TTPs (tactics, techniques, and procedures) with geopolitical events, newly disclosed vulnerabilities, or sector-specific risk patterns. Others use graph-based reasoning to uncover previously hidden connections between indicators of compromise (IOCs) and attacker infrastructure. For example, identifying that a new domain seen in phishing campaigns shares hosting characteristics with infrastructure used by a known APT group.

# Section 4- From Static Defenses to Self-Evolving Systems: The Security Practitioner's AI Imperative

For the security practitioner, this means shifting from "What just happened?" to "What's likely to happen next?", a fundamental improvement in how we prioritize limited resources.

**Natural Language Processing (NLP) for Cyber Defense**
Security data is messy. Much of it, whether vulnerability disclosures, threat reports, incident tickets, or user emails is unstructured data. Natural Language Processing (NLP) allows defenders to parse, correlate, and make sense of this flood of human language data.
NLP models can extract entities (e.g., IP addresses, CVE numbers, file hashes) from threat intel reports, normalize them, and feed them into detection rules or enrichment pipelines. In vulnerability management, these models can summarize patch guidance, map it to asset inventories, and generate context-aware risk scores for remediation prioritization.

Some platforms are now integrating conversational AI into ticketing systems, allowing analysts to interact with log data using natural language prompts ("Show me all failed login attempts from foreign IPs in the last 24 hours"), reducing the time spent writing complex queries. Others use NLP to automatically classify phishing emails, identify brand impersonation, or even translate attacker messages scraped from forums and pastebins.

**Automated Incident Response**
Time-to-response is often the difference between a minor incident and a breach. AI-driven SOAR (Security Orchestration, Automation, and Response) platforms are now capable of triaging alerts, correlating them with related activity, and taking containment actions – all without human intervention.

For example, upon detecting an anomalous login, an AI-driven system might check whether the IP is known malicious, examine the user's recent activity for anomalies, and then quarantine the device, revoke tokens, or disable the account. This doesn't replace human analysts, but it gives them breathing room to focus on higher-level investigations and strategic initiatives.

Automation also helps reduce alert fatigue. By learning from analyst responses, AI models can prioritize incidents that are likely to be true positives, improving analyst efficiency and morale in high-volume environments.

**Digital Forensics and Threat Hunting**
AI is also transforming post-incident analysis and proactive threat hunting. In digital forensics, AI can surface relevant artifacts from massive datasets such as registry changes, file modifications, or anomalous process executions based on learned patterns from prior incidents.

For threat hunters, AI can generate hypotheses based on behavioral outliers, helping guide investigations toward likely indicators of compromise. For example, a model might identify a rarely used account that initiated RDP sessions to multiple endpoints, or correlate registry activity that resembles known malware staging behavior.

Some platforms now provide AI-assisted investigation timelines, automatically stitching together attacker activity across logs, endpoints, and cloud events to create a coherent narrative. This dramatically reduces the time required to reconstruct incident chains and identify root cause.

### AI in Red Team and Blue Team Operations

As AI transforms real-world threats and defensive capabilities, it is also reshaping how cybersecurity teams train, simulate, and validate their readiness. Within red and blue team operations, AI is being integrated to improve realism, speed, and scale, enabling more effective emulation of adversary tactics, while also enhancing defenders' ability to detect, respond, and learn in live-fire or tabletop scenarios. Security teams are no longer limited by static rules or canned simulations; AI is opening the door to dynamic, adaptive engagements where both attackers and defenders can think and act at machine speed.

#### AI-Augmented Red Teaming

Red teams traditionally rely on manual reconnaissance, payload development, and exploitation to simulate realistic threats. With AI, many of these phases can now be accelerated and enhanced. Language models can assist in crafting highly convincing spear-phishing messages or pretexts tailored to the target's organization, region, or role. These messages can be generated in real time, responding to defender prompts or simulated help desk conversations.

AI can also be used to automate parts of the kill chain. For example, generative code models can assist in modifying malware to evade specific endpoint detection tools or mutate shellcode to bypass heuristic-based firewalls. In more advanced red team engagements, reinforcement learning agents are being trained to navigate target networks, adjust tactics based on detection signals, and even pivot through misconfigured APIs or SaaS platforms all without pre-programmed logic.

This increases the realism of exercises and helps CISOs validate whether detection and response controls can stand up not just to known TTPs, but to novel, evolving techniques that resemble how AI-assisted adversaries behave.

# Section 4- From Static Defenses to Self-Evolving Systems: The Security Practitioner's AI Imperative

**AI-Powered Deception and Honeypots**
On the defensive side of simulation, blue teams are beginning to deploy AI-enhanced honeypots and deception systems that evolve in response to attacker behavior. Traditional honeypots can be easily fingerprinted or bypassed. AI-powered deception platforms, by contrast, can generate realistic user activity (logins, file access, browsing behavior), update fake credentials or decoys, and adapt network or system configurations to maintain plausibility over time.

When an attacker interacts with an AI-managed honeypot, the system can respond with dynamic content such as synthetic documents or fake Active Directory structures designed to capture TTPs, delay lateral movement, and alert defenders early. Some deception frameworks are also integrating NLP-driven bots that simulate end-user or helpdesk interactions, further increasing believability and engagement.

This adds an active layer to defense-in-depth strategies: not just detecting compromise but actively shaping adversary behavior and collecting high-fidelity telemetry in the process.

**AI for Enhanced Blue Team Operations**
Beyond simulations, AI is becoming a daily operational asset for blue teams. AI models are being embedded in SIEM and XDR platforms to automatically cluster related alerts, identify attack patterns across multiple sources, and prioritize threats based on contextual risk.

Rather than parsing raw logs manually, blue teams can now use AI to extract behavioral baselines and highlight deviations that might signal insider threats, lateral movement, or staging behavior. These systems can identify complex correlations such as a rarely used service account that accessed sensitive files and initiated outbound DNS tunneling within the same session.

In a live incident, AI helps defenders cut through noise. It can surface the "storyline" of the attack by linking processes, accounts, IP addresses, and assets in a coherent timeline. This reduces investigation time and improves the quality of incident response reports.

As AI models learn from confirmed incidents and team feedback, they become increasingly effective at recommending playbooks, mitigation steps, or enrichment queries. This is especially valuable in lean SOC environments where human resources are stretched.

# Section 4- From Static Defenses to Self-Evolving Systems: The Security Practitioner's AI Imperative

**Training and Simulation**

AI is also transforming how security teams train. Traditional tabletop exercises or red vs. blue simulations often rely on static injects and human facilitation. AI-enabled training platforms can now create adaptive scenarios where the attack narrative evolves based on participant responses.

For example, if a blue team detects and blocks an initial attack vector quickly, the AI can shift to a different TTP (e.g., credential stuffing or supply chain compromise), forcing defenders to remain engaged and flexible. This allows for higher-fidelity testing of escalation paths, communication protocols, and cross-functional coordination in real time.

AI can also serve as an intelligent adversary in wargaming simulations, testing a team's readiness against a variety of threat actor profiles, each with distinct motivations, resources, and techniques. Some platforms are beginning to integrate LLMs as virtual participants such as end users, threat actors, or even simulated media and public relations responses to enrich scenarios beyond technical containment.

These training advancements not only improve technical readiness but also help teams practice decision-making under pressure which is an essential component of mature cyber resilience.

### Ethics, Privacy, and Bias in Security-Focused AI

As AI becomes more deeply integrated into security operations, it also introduces a range of ethical, legal, and social challenges that cannot be ignored. These include systemic bias in AI models, the risks of data misuse or overcollection, the ethical implications of offensive automation, and the need for transparency in automated decision-making. Security teams face a dual responsibility: not only to deploy AI effectively, but to do so in a way that respects user rights, aligns with evolving regulatory requirements, and earns the trust of stakeholders. Governance is no longer optional; it is foundational to sustainable AI adoption.

**Bias in Security Algorithms**

Even in cybersecurity, bias can emerge in unexpected ways. AI models trained on historical security data may learn to overrepresent certain behaviors, roles, or geographic origins as "risky" based on incomplete or skewed training sets. For example, a user from a non-U.S. IP address logging into a system outside of business hours may be flagged as anomalous even if that user is a remote contractor or researcher working across time zones.

Similarly, user behavior analytics (UBA) systems may unfairly target employees with less consistent schedules or usage patterns, such as faculty, shift workers, or those in accessibility programs. If these models are tuned only to detect deviation from the majority, they may miss subtle indicators of compromise while producing noisy, biased false positives.

Without regular audits, these biases can become embedded in detection pipelines, producing alerts that are not just ineffective but inequitable. Security teams must adopt practices like fairness testing, adversarial validation, and diverse training datasets to minimize these risks – and they must do so proactively, not reactively.

**Data Privacy and Regulatory Compliance**
Security AI often requires vast quantities of data, from system logs and identity events to endpoint telemetry and email content. The collection, retention, and use of this data raise serious privacy and compliance concerns, especially in sectors like healthcare, higher education, and government.

AI models trained on sensitive content such as emails, chat transcripts, or research data may inadvertently expose or replicate personally identifiable information (PII) or protected health information (PHI). In environments subject to FERPA, HIPAA, GDPR, or state-level privacy laws, improper data handling could lead to regulatory penalties, civil liability, or reputational damage.

Security practitioners must ensure that AI tooling aligns with data minimization principles, role-based access controls, and proper encryption both at rest and in transit. It's also critical to understand how third-party AI vendors process customer data, whether model training is isolated per tenant, and how long logs or model artifacts are retained. These concerns are especially important when integrating AI into cloud-native platforms or productivity suites.

Clear internal documentation and cross-functional governance with legal, privacy, and compliance teams are essential. Security leaders must view themselves not just as tool implementers, but as stewards of sensitive data.

**Transparency and Accountability**
One of the biggest operational risks in AI-assisted security is opacity. Many AI models, especially deep learning-based ones, lack explainability. When an AI system flags an alert, disables a user, or quarantines an endpoint, defenders must be able to understand why the decision was made.

Without this transparency, SOC analysts may struggle to validate results, reproduce findings, or respond to stakeholder inquiries. This becomes even more problematic in environments where security decisions may have legal, HR, or academic consequences.

To mitigate this, organizations should prioritize tools that provide interpretable models or “explanation layers” that expose model logic, contributing features, or rule thresholds. Logging and decision auditability are also essential – not just for debugging, but for internal accountability and external reviews.

Moreover, governance frameworks should include escalation paths, overrides, and review processes to ensure that AI-driven actions remain subject to human oversight.

**Ethical Use of Offensive AI**

Red team operators are increasingly using AI to simulate sophisticated threats, craft convincing phishing content, and automate aspects of offensive engagements. While these practices improve realism and preparedness, they also raise ethical questions.

For example, should a simulated phishing campaign use AI to impersonate a real executive? What are the boundaries for generating synthetic content that could cause reputational or psychological harm – even in training? Should there be restrictions on using uncensored LLMs in adversarial testing environments?

Security teams must ensure that their offensive tooling is guided by clear policies, ethical review processes, and (when relevant) participant consent. Just because something is technically feasible doesn’t mean it should be deployed indiscriminately. AI red teaming must remain grounded in risk-aware design, especially when operating within academic, nonprofit, or healthcare institutions where mission alignment and ethical integrity are paramount.

Organizations may also consider establishing internal AI Acceptable Use Policies (AUPs) that govern both defensive and offensive use of generative models. These frameworks can clarify what types of data can be fed into LLMs, how outputs may be stored or reused, and who retains accountability for outcomes.

**Exercises and Governance Prototypes**

Security leaders should routinely test their teams’ awareness of ethical risks through tabletop exercises and prompt injection challenges. For example, teams might evaluate how different AI tools respond to gray-area queries, such as generating phishing content or providing instructions for exploiting a known CVE. Comparing responses from models with and without safety filters can spark valuable discussion.

# Section 4- From Static Defenses to Self-Evolving Systems: The Security Practitioner's AI Imperative

Institutions should also begin drafting AI governance templates that align with their unique missions. These policies should address issues like prompt confidentiality, model fine-tuning restrictions, vendor accountability, and disclosure protocols in the event of AI-driven incidents. The goal is not to stifle innovation, but to provide clear guardrails in a fast-moving environment.

Across the U.S., AI governance is still in its early stages, especially within security programs. But early adopters are beginning to form internal councils, tie AI usage policies to their broader risk management frameworks and treat AI use as a board-level concern. Security practitioners must take the lead in ensuring that AI is not only effective but responsible, lawful, and just.

### Securing AI Systems: Defenses Against AI-Specific Threats

As organizations increasingly rely on AI to power core security and business functions, the systems that deliver AI capabilities become new targets themselves. From poisoning model inputs to tampering with training pipelines or attacking model APIs, threat actors are already probing AI systems for weaknesses. Defending these systems requires a shift in mindset, from viewing AI solely as a tool for security to recognizing it as an infrastructure layer that must be secured like any other high-value asset. This section focuses on the unique threats to AI systems, and the strategies practitioners can adopt to mitigate them.

**Model Security and Robustness**

Machine learning models – especially those exposed via public or partner-facing APIs – can be attacked directly. Adversaries may attempt model evasion, submitting specially crafted inputs designed to trigger incorrect outputs. These manipulations often exploit subtle quirks in the model's learned patterns, allowing malicious input to bypass detection.

More targeted threats include model extraction, where an attacker queries a model repeatedly to reconstruct its logic and reproduce it offline. This can be used to steal proprietary models or to build surrogate models for crafting adversarial inputs.

To address these risks, defenders can implement input validation, rate limiting, and detection of abnormal query patterns, particularly for APIs exposed externally or across organizational boundaries. Some platforms now include adversarial robustness testing features that evaluate whether small input perturbations cause unacceptable drift in output behavior. Security teams should treat this as part of routine pre-production hardening for models integrated into sensitive workflows.

Where possible, models should be wrapped in protective layers that log access, perform sanity checks on inputs and outputs, and isolate critical decisions from being executed without human review.

# Section 4- From Static Defenses to Self-Evolving Systems: The Security Practitioner's AI Imperative

**Data Integrity and Poisoning Defense**
Because AI models learn from the data they're trained on, poisoning that data can distort their predictions in subtle and dangerous ways. This is especially problematic in environments that retrain models continuously using live input (e.g., anomaly detection pipelines or adaptive endpoint models).

An attacker who introduces mislabeled or maliciously crafted data into the training stream can cause a model to misclassify critical events or even learn to ignore certain types of threats entirely. Poisoning can occur through upstream compromises (e.g., corrupting log sources, manipulating alert labels), through supply chain attacks, or by compromising trusted third-party datasets.

Defenders must apply the same data governance rigor to model inputs that they do to structured systems. This includes access controls, data provenance tracking, input validation, and segregation of training vs. test data. In high-risk environments, practitioners should consider differential privacy techniques or trusted execution environments (TEEs) for model training workflows, especially when training on sensitive or proprietary datasets.

Teams should also monitor for label drift and anomalous training set characteristics, which can indicate poisoning attempts or unintended data leakage.

**Securing AI Infrastructure**
The infrastructure that supports AI workloads such as cloud compute environments, storage pipelines, orchestration tools, and model registries must be secured like any other production system. Unfortunately, in many organizations, AI infrastructure is managed by data science or DevOps teams with limited involvement from information security.

Common misconfigurations include open S3 buckets storing training data, overly permissive IAM roles granting access to GPU clusters, unpatched model-serving containers, and API keys embedded in notebooks or automation scripts. These gaps expose not only models and data, but the underlying platforms that attackers could leverage for lateral movement or cryptojacking.

Security teams should integrate AI infrastructure into existing cloud security posture management (CSPM) programs and vulnerability management cycles. Baseline configurations for model-serving infrastructure should include hardening guides, network segmentation, and container scanning.

# Section 4- From Static Defenses to Self-Evolving Systems: The Security Practitioner's AI Imperative

It's also essential to monitor changes to models, configuration files, and dependency libraries. Just as organizations track changes in source code and CI/CD pipelines, they must now monitor model versioning, data pipeline changes, and training script integrity to detect tampering or drift.

**Continuous Monitoring and Testing of AI Models**
AI systems are not static, they evolve. Their performance can degrade over time due to data drift, changes in user behavior, emerging attack techniques, or feedback loops. Without continuous monitoring, even a well-trained model can become a liability.

Practitioners should implement monitoring tools that track model output distributions, false positive/false negative rates, and decision latency across different environments and user groups. Unexpected spikes or shifts in these metrics may indicate concept drift, degradation, or manipulation attempts.

For high-stakes applications such as fraud detection, malware classification, or access anomaly detection, organizations should maintain a testing regimen that includes shadow deployment (where a new model runs in parallel without impacting production), canary releases, and automated regression testing. Some teams now use AI itself to generate adversarial test cases or simulate edge conditions that might cause failure.

Finally, just as penetration testing and red teaming are common for traditional infrastructure, organizations should begin adopting AI-focused security assessments that evaluate not just application vulnerabilities, but model-specific weaknesses, data pipeline hygiene, and the completeness of their AI incident response plans.

### Future Directions: Emerging Trends and the Role of AI in Security

The intersection of artificial intelligence and cybersecurity is still in its early stages, but the pace of innovation is accelerating. As generative models become more capable, infrastructure becomes more modular, and attackers more adaptive, the role of AI in both offensive and defensive security is likely to deepen and diversify. Security practitioners must not only respond to current threats but anticipate how emerging capabilities – and emerging risks – may shape the next wave of digital conflict and control. This section explores several frontier areas where AI and security are converging, raising new questions about readiness, governance, and opportunity.

# Section 4- From Static Defenses to Self-Evolving Systems: The Security Practitioner's AI Imperative

**AI and Quantum Computing**

Although still largely experimental, the convergence of AI and quantum computing has the potential to reshape cryptography, optimization, and threat analysis. Quantum machines could eventually accelerate AI model training and inference, reducing cost and increasing accessibility of capabilities that today require hyperscaler-level infrastructure. Conversely, AI can help optimize quantum algorithms and resource allocation, allowing more efficient simulations and scheduling in complex computing environments.

From a security perspective, quantum-AI synergy could impact:

- Cryptanalysis: AI could assist quantum systems in modeling attack paths against cryptographic algorithms, especially those not yet quantum resistant.
- Behavioral modeling: Quantum-enhanced AI may eventually model attacker behavior more effectively than classical systems, improving prediction in threat intel and fraud prevention.
- Optimization in red/blue operations: AI could help quantum machines identify optimal lateral movement paths or most vulnerable nodes in simulated attack graphs.

While practical deployment is years away, organizations involved in high-value research, defense, or critical infrastructure should begin tracking these trends and evaluating the implications of post-quantum readiness alongside AI strategy.

**The Role of Generative AI in Future Threats**

Generative AI, especially large language models (LLMs), text-to-image, and voice synthesis tools will likely remain the most active area of concern soon. As model quality improves and open-source access widens, threat actors will gain the ability to generate:

- Convincing real-time phishing and business email compromise (BEC) content
- Deepfakes of public figures, executives, and law enforcement officials
- Synthetic voice impersonations for vishing and multi-factor authentication bypass
- Realistic documentation (IDs, invoices, contracts) for fraud and social engineering

The barrier to running these tools is dropping rapidly. What once required access to private GPUs and AI engineering expertise is now achievable via web-based APIs or downloadable models that can be fine-tuned for specific scams or adversary campaigns.

Defenders must consider how generative AI will not only improve attacker efficiency but also erode trust in digital authenticity. Traditional anti-phishing training, executive impersonation alerts, and document validation methods must be revisited through this new lens.

# Section 4- From Static Defenses to Self-Evolving Systems: The Security Practitioner's AI Imperative

**Human-Machine Collaboration**
As AI tools proliferate, practitioners are increasingly operating in co-pilot mode, using AI to assist with triage, correlation, hunting, and reporting. The future of cybersecurity is not AI versus human, but human + AI versus machine-augmented adversaries.

In the SOC, we're already seeing use cases where LLMs summarize alerts, generate investigative queries, and assist with writing post-incident reports. Threat hunters are using AI to process months of telemetry in minutes. Red teams are crafting payloads with generative assistance. Executives are asking AI to explain risk trends and remediation metrics in plain English.

But this collaboration requires guardrails. Without proper training and oversight, teams may become over-reliant on AI-generated insights, miss adversarial manipulation of AI outputs, or introduce new risks via careless prompt engineering or data exposure.

Security leaders should invest in workflows where AI augments human skill rather than replaces it. This includes training analysts to validate AI output, explain model behavior, and know when to override automated decisions.

**Investment in AI for Cybersecurity**
The current state of AI adoption in cybersecurity resembles an early adopter phase. Most organizations are cautiously experimenting by integrating AI-powered features from existing vendors, testing copilots in low-risk domains, and exploring open-source models in sandboxed environments. Use cases are growing, but strategic maturity remains limited.

However, early indicators suggest that AI-native security platforms designed from the ground up with machine learning at the core will begin to disrupt traditional vendors in the next 18–24 months. These platforms may offer:

- Autonomous detection-and-response loops that bypass manual escalation
- Full-log ingestion with semantic summarization and contextual linkage
- Customizable model stacks tailored to the organization's unique environment

Security programs that invest now by upskilling staff, establishing governance, and piloting AI use cases will be better positioned to capitalize on these capabilities when they mature. For many, the next phase will involve formalizing AI governance committees, establishing AI readiness assessments, and adopting a security-as-code approach to AI configuration and deployment.

# Section 4- From Static Defenses to Self-Evolving Systems: The Security Practitioner's AI Imperative

Maintaining a competitive advantage will depend not only on tooling, but on how well organizations align AI initiatives with broader risk management, compliance, and workforce development strategies.

### Conclusion & Recommendations: Preparing the Cybersecurity Workforce for an AI-Augmented Future

As artificial intelligence reshapes the security landscape, from attack tactics to defensive operations, it is also redefining the roles, responsibilities, and required skillsets of the cybersecurity workforce. The practitioner's mindset must evolve from rule-based thinking to pattern recognition; from manual response to automated orchestration; from static roles to continuous reskilling.

Security leaders must act now to ensure their teams are not only equipped to operate in an AI-enabled environment but are prepared to lead it. The following recommendations merge operational priorities with strategic workforce development to future-proof cybersecurity programs in the AI era.

1. **Integrate AI Threats into Skills Training and Playbooks** – Adversarial AI, deepfakes, automated phishing, and synthetic identities are no longer emerging threats, they are here. Incorporate these risks into existing playbooks, incident response training, and workforce readiness assessments. Analysts, responders, and red teamers must know how to identify, simulate, and counter AI-driven attacks as a core competency.

2. **Reskill Analysts to Collaborate With, Not Just Use, AI** – The analyst of the future won't just use AI; they'll co-pilot investigations with it. Train SOC and IR personnel to interpret AI-generated alerts, validate machine-curated narratives, and identify edge cases where human judgment is essential. Fluency in prompt engineering, model feedback loops, and explainability will become critical job functions, not fringe skills.

3. **Secure AI Systems and Build Talent to Do It** – Securing AI pipelines and model infrastructure introduces entirely new domains: model robustness testing, adversarial red teaming, data integrity validation, and AI-specific incident response. Begin upskilling your cloud security, DevSecOps, and GRC staff on these domains or partner with academic institutions to cultivate the next generation of AI-literate defenders.

4. **Build Ethical and Governance Literacy into Every Role** – AI ethics, privacy, and policy cannot be siloed. Frontline staff must understand data minimization, bias mitigation, and responsible AI use, especially when handling sensitive prompts, labels, or generated content. Establish internal AI governance frameworks that define role-based responsibilities for compliance, transparency, and accountability.

# Section 4- From Static Defenses to Self-Evolving Systems: The Security Practitioner's AI Imperative

5. **Invest in AI-Enhanced Training and Simulation Platforms** – Replace static tabletop exercises with adaptive, AI-driven simulations that reflect real-world adversary behavior and evolving threat scenarios. Leverage LLMs to generate dynamic injects, user personas, and narrative evolution. These tools aren't just force multipliers for attackers, they're also powerful accelerants for team learning and preparedness.

6. **Design Career Paths for AI-Enabled Roles** – New roles are emerging, AI Risk Analyst, Prompt Security Engineer, ML Security Auditor, AI Threat Intelligence Analyst. Begin to define internal career paths that support these capabilities. Partner with HR, academic institutions, and vendor partners to forecast future workforce needs and offer certifications, fellowships, or apprenticeships focused on security + AI.

The cybersecurity workforce is at an inflection point. As automation handles more of the volume, the value of human defenders will come from their ability to guide, challenge, and safeguard AI systems, not just use them. The organizations that thrive will be those that treat workforce development as a strategic pillar of AI adoption, not an afterthought. Security practitioners must become not only AI adopters but AI architects, translators, and ethicists. The time to build that future-ready workforce is now.

# Section 5- Artificial Intelligence Legislation, Governance, and Oversight

By Emily Harris, JD, CISSP, CIPP/US, Chief Information Security Officer (CISO) at Montclair State University, Montclair, NJ.

### Introduction

The broad adoption of cutting-edge technology naturally gives rise to legislation and regulations that seek to both accelerate innovative uses of new technology and implement controls around its development and use to mitigate known and unknown risks. The United States is a forerunner of technology innovation and adoption. As stated by the White House Executive Order issued on January 23, 2025, the United States strives to become a global leader in Artificial Intelligence by declaring "[i]t is the policy of the United States to sustain and enhance America's global AI dominance." [31] At the same time, both the 118th and 119th Congress have introduced multiple bills

[31] *Executive Order 14179,* The White House, https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/ (Jan. 23, 2025).

that regulate various aspects of AI, including its development, deployment, and usage. Although Congress has not yet passed comprehensive federal legislation, individual states have introduced and passed legislation to address AI risks. In addition, the European Union recently passed the EU AI Act, which will be fully applicable in 2027.

This report discusses the risks AI poses, including use by malicious actors, cybersecurity concerns, data privacy, and potential discriminatory and unethical impacts. Legislation attempts to mitigate these risks in different ways. Some provisions ban the use of AI for specific purposes. Others require that features are added during the development of AI systems and models to mitigate specific risks, such as preserving data integrity in model training or cybersecurity controls based on industry standards and frameworks. Some legislation prevents the use of media produced by generative AI in certain circumstances, for example, to protect minors and preserve election integrity.

Understanding the current and potential future legislative and regulatory environment is important to create meaningful curriculums for an AI-ready workforce. During educational programs, sound practices in secure software development, building in key features and technologies, and creating clear explanatory documentation will create a workforce ready to address such requirements in both public and private industries.

## Summary Overview of European Union and United States Artificial Intelligence Legislation

### Themes in EU and State Regulations

Both the EU AI Act and proposed and enacted state legislation have provisions based on common themes and risks:

1. **Innovation** – AI can have a positive effect on society, contributing to new ways to address complex social problems including climate change, improving health care outcomes, and criminal justice reform. This theme stresses the importance of encouraging innovation, supporting research and development in new AI models, and striking a balance between mitigating prospective harms and fostering creativity.

2. **Governance** – Specifies a framework for creating policy, procedures, and oversight related to AI system deployment and AI model training. This includes creating new agencies, boards, or working groups with designated personnel and clear reporting structures. These provisions also include direct AI governance requirements, such as impact assessments and AI model registration. Governance sets up requirements related to all the other themes.

3. **Risk Management** – High-risk AI requires evaluating and mitigating risks of harm from its use. These provisions define high-risk systems and create specific requirements for those systems which have the greatest risk of adverse negative impacts to individuals and society at large. The risk management requirements often include rules for categorizing AI as high-risk, regular assessments of the risk of AI, impact assessments, and adopting industry standards and frameworks.

4. **Accountability and Responsibility** – This establishes which companies, organizations, or individuals develop or deploy AI. They need to supply contact information to government bodies for compliance and communication. This helps these bodies enforce provisions, creates AI inventories, and contributes to preventing illegal or unapproved AI systems from being deployed.

5. **Transparency** – A critique of AI models is that they are "black-box." AI users do not know how they work, deployers don't have visibility into how developers created the systems, and developers themselves may not understand how a mature AI makes its inferences and decisions. This theme also includes user consent and notification, where those interacting with AI or using it for automated decisions or outcomes need to consent to its use, be notified that their interactions are with an AI, or both. Notification requirements also include those to AI governance bodies or Attorneys General, for both regulatory documentation and incident response. In terms of generative AI, transparency relates to watermarks or disclosures clearly displayed on AI-generated content.

6. **Anti-discrimination** – Provisions that require diversity in training models so that they include data from underrepresented minorities, meant to prevent discrimination in automated decision-making. Other provisions provide protections against discriminatory outcomes that could have harmful results to individuals.

7. **Human oversight** – These provisions include two components: 1) the option for an individual to opt-out from automated decision-making and invoke the right to have a human make the decisions instead; and 2) human checks on AI system outcomes and decisions, to verify they are not erroneous or discriminatory.

8. **Cybersecurity and Data Protection** – These provisions keep AI systems and models safe from unauthorized access or cyber attackers. They help 1) protect from infiltration; 2) ensure AI systems stay available; 3) prevent training data poisoning; and 4) prevent tampering intended to change algorithmic decision-making and outcomes. If a bad actor infiltrates an AI system and changes the algorithm, there could be detrimental, harmful results. These provisions also protect training data and outcomes, which could include personally identifiable information. They also protect trade secrets, copyrights, patented technology and proprietary corporate assets.

# Section 5- Artificial Intelligence Legislation, Governance, and Oversight

9. **Privacy** – This addresses both the data used for model training, and the protection of the automated decisions or outcomes if they include sensitive data of individuals. The primary emphasis is on training data, and ensuring that personal data is anonymized, or consent is obtained before using personal data for training.

10. **The "Kill Switch"** – The worst-case scenario for AI is a system that becomes self-aware and begins acting independently from human operators, making decisions based on flawed or unreasonable logic and leading to significant harm (like the SkyNet scenario from Terminator). These provisions include variations of a "kill switch" requirement, which can terminate the operation of an AI system or model if 1) it does not adhere to regulations; 2) the AI system causes a significant incident resulting in imminent or active harm; or 3) there is an event requiring investigation.

All these themes appear in the EU AI Act. Many of these themes also appear in enacted and proposed U.S. federal and state legislation.

### The EU AI Act

The European Commission first conceived of a European Union AI Act in 2021. An earlier EU Act, the GDPR, which became applicable on May 25, 2018, included provisions requiring consent and transparency for applications making use of automated decision making. [32] Early drafts of the EU AI Act were significantly revised after the launch of ChatGPT in 2022 to accommodate the acceleration of AI adoption. The European Parliament passed the EU AI Act on March 13, 2024 and the European Council approved it on May 21, 2024. The complete Act becomes applicable on August 2, 2027. Key provisions are already applicable, including prohibitions on certain AI systems and governance requirements for member states. [33]

The scope of the Act includes providers and deployers located in the EU, and any AI that impacts a citizen of the EU. This means that both United States technology companies that develop AI and private and public industries with clients, customers, or students in the EU have to comply with the substantive provisions of the Act. Understanding the impact of the provisions helps companies and researchers build in key features into the earliest stages of development.

[32] GDPR Art. 22(1), https://gdpr-info.eu/art-22-gdpr/ (2016).

[33] *EU Artificial Intelligence Implementation Timeline, Future of Life Institute, https://artificialintelligenceact.eu/implementation-timeline/*

# Section 5- Artificial Intelligence Legislation, Governance, and Oversight

### Structure of the Act

The EU AI Act Article 3(1) defines an AI system as having five characteristics: 1) the system is machine-based; 2) it has some level of autonomy; 3) it may adapt after deployment; 4) the system makes inferences; and 5) it can influence "physical and virtual environments." Recital 12 further explains that an AI system's capability to infer is a "key characteristic," differentiating it from other automated systems. [34]

The Act specifies different requirements for different types of technologies. An AI system is any software or device that meets the definition above. It can operate as its own software for a single purpose, as a component of a larger software platform or service, or can be embedded into devices for a specific propriety operation (for example, factory equipment automation or medical devices). A general-purpose AI system is an AI system based on a model that has the capability to serve a variety of purposes, both for direct use and integration in other AI systems. [35] Most provisions in the Act are only applicable to high-risk AI systems, which are those that are used as safety components in other products [36] or those specifically defined by the Act. [37] The Act does not specifically cover media produced by generative AI, but considers generative AI a type of general-purpose AI system. [38] Some uses of AI are outright prohibited, including using deceptive or manipulative tactics to impair an individual's decision-making ability, exploiting a person's vulnerabilities to manipulate behavior, using AI to classify people into categories or profile them to evaluate the risk of future criminal behavior, types of facial identification, and certain uses of biometrics. [39] Many of the prohibitions have exceptions for public safety, public health, and law enforcement activities. [40]

### Key Requirements

The following requirements are a sample of prominent provisions in the EU AI Act as they relate to the common themes of AI legislation listed previously.

Innovation:

- Creates AI regulatory sandboxes to foster innovation in an environment that meets Act's regulatory requirements.

[34] The OECD definition of AI explicitly states that an AI System "infers, from the input it receives, how to generate outputs…". *OECD AI Principles Overview,* OECD.AI Policy Observatory, https://oecd.ai/en/ai-principles. The United States definition of AI is less direct, including in its definition of AI that AI systems "use machine and human-based input to…use model inferences to formulate options for information or action." *National Artificial Initiative Act of 2020, Congress.gov*, https://www.congress.gov/bill/116th-congress/house-bill/6216/text.

[35] EU AI Act Art. 3 § 63.

[36] EU AI Act Art. 6 § 1(a).

[37] EU AI Act Art. 6 §2.

[38] EU AI Act Recital 99.

[39] EU AI Act Art. 5.

[40] *Id.*

# Section 5- Artificial Intelligence Legislation, Governance, and Oversight

General Governance:

- Establishes the AI Office which sits within the EU Commission.
- Designates national authorities within member states.

High-Risk AI requirements for providers: [41]

- **Governance** – technical documentation to demonstrate compliance and provide authorities with the necessary information to assess that compliance; establish a quality management system to ensure compliance; registration and certification.
- **Risk Management** – establish a risk management system throughout the high risk AI system's lifecycle.
- **Accountability and Responsibility** – company name, authorized representative, details of the AI system, and other information to be submitted as part of the registration process.
- **Transparency** – provide instructions for use to downstream deployers.
- Anti-discrimination – ensuring that training, validation and testing datasets are relevant and sufficiently representative.
- **Human oversight** – design the AI system to allow deployers to implement human oversight.
- **Cybersecurity and Data Protection** – build in resiliency measures to prevent cyber-attacks or the negative harm resulting from one; design and develop systems with appropriate levels of cybersecurity; ensure that training, validation and testing datasets are free of errors and complete according to the intended purpose.
- **Privacy** – limit the use of personal information for processing, except in specific circumstances.
- **"Kill Switch"** – build a stop button or similar procedure to allow the system to be fully halted safely.

General-purpose AI:

- **Governance** – Track, document and report serious incidents and possible corrective measures to the AI Office and national competent authorities.
- **Risk Management** – assess and mitigate possible systemic risks, including their sources.
- Accountability and Responsibility – designate an authorized representative to interact with the AI Office; provide contact information for the provider to EU authorities.
- **Transparency** – draw up technical documentation, including training and testing process and evaluation results; documentation sufficient to give downstream providers an understanding of the AI's capabilities and limitations.
- **Anti-discrimination** – publicly publish a sufficiently detailed summary about the content used for training.
- **Cybersecurity and Data Protection** – perform model evaluations, including conducting and documenting adversarial testing; ensure an adequate level of cybersecurity protection.

[41] *See generally* EU AI Act.

# Section 5- Artificial Intelligence Legislation, Governance, and Oversight

### United States Artificial Intelligence Legislation

The U.S. Government, Puerto Rico, and a majority of states have enacted legislation or proposed bills that regulate aspects of generative artificial intelligence, algorithmic decision-making, AI generated media, and AI systems. Most of this legislation is sectoral, focusing on the use of AI in government, healthcare, finance, education, and other industries. Legislatures have also made amendments to existing legislation to accommodate advancements in AI, including amending election legislation to prohibit the use of deep fakes in campaigning and amending criminal codes to criminalize the use of AI-generated content depicting minors in sexual acts. A minority of states have enacted or proposed broad, generalized AI legislation that either provides consumer protections to their residents or creates governance bodies, policies and procedures to oversee AI use in the state. Most states that have enacted such legislation have existing privacy laws that now have new provisions requiring that consumers have options to opt-out from having personal information used for training or profiling and automated decision-making. This year, there are over 100 proposed AI bills in New York, Illinois, California, Maryland, and Texas alone. [42]

### Comprehensive State AI Legislation

Colorado, Texas, and Utah are the only states with enacted comprehensive AI legislation addressing consumer protection and AI governance. All three states have provisions referencing themes of innovation, governance, and transparency.

Colorado has the most comprehensive legislation, with provisions across all themes except accountability and responsibility, human oversight, and cybersecurity and data protection, and a "kill switch." Of the three, only Utah specifies cybersecurity and data protection requirements, but only on the state's Learning Lab, a sandbox environment for research and development of new and innovative AI.

The most comprehensive state AI bill to date was California's Safe and Secure Innovation for Frontier Artificial Intelligence Models Act, proposed and passed in 20224. However, the Governor vetoed the bill, which prompted lawmakers to take a more piecemeal approach by amending current laws and enacting industry-specific legislation. [43] New York currently has comprehensive proposed legislation titled the New York Artificial Intelligence Bill of Rights, initially proposed in 2024 and now carried over into 2025. [44]

### State Sectoral Legislation and Amendments

All fifty states except Wyoming, Missouri, and Ohio have AI legislation either related to a particular sector or embedded into other laws. [45] For example, Oklahoma amended their distribution of intimate images and CSAM laws to include AI-generated sexual content. [46] Mississippi passed legislation prohibiting AI deep fakes from being used in political advertising. [47] New York amended N.Y. Civil Rights Law Section 50 to extend individual privacy rights to AI-generated uses of the

[42] *How Different States are Approaching AI, Brookings,* https://www.brookings.edu/articles/how-different-states-are-approaching-ai/ (Aug. 18, 2025).

[43] *Id.*

[44] *Assembly Bill A3265, The New York State Senate,* https://www.nysenate.gov/legislation/bills/2025/A3265 (2025).

[45] *Loeb & Loeb 2025 U.S. State AI Legislation Tracker, Loeb & Loeb, LLP,* https://www.loeb.com/en/general/ai (last updated Jul. 1, 2025).

individual's likeness, picture, or voice. [48] New York City Employment Law 144 creates requirements that any government agency using automated decision making in screening candidates for employment include the ability of a candidate to opt-out. [49] Arizona requires a human being to review the denial of a medical claim based on medical necessity, and objectively review the claim without relying on other inputs, including algorithms. [50] Effective January 1 2026, Nebraska will require that consumers can opt-out of having their personal data used in automated decision making related to certain attributes and outcomes. [51]

Other states amended their consumer privacy laws to add language related to profiling or automated decision-making. The Florida Digital Bill of Rights now includes the requirement that a consumer has a right to opt-out of the processing of personal data for the purposes of "profiling in furtherance of a decision that produces a legal or similarly significant effect." [52] The Montana Consumer Privacy Act contains a similar provision, granting a consumer the right to opt-out of processing their personal data for "profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer." [53] Other states with similar language in consumer privacy laws include Nebraska, New Hampshire, Oregon, Indiana, Connecticut, Tennessee, and Virginia. [54]

### Summary

The EU AI Act is comprehensive legislation that seeks to promote innovative uses of AI while protecting EU citizens from the anticipated and unanticipated risk of harms arising from AI use and adoption. United States public and private organizations should understand the impact of the law on their own development of AI systems intended for use in the EU or by EU citizens. The EU GDPR had a meaningful impact on how U.S. organizations secured their technologies and honored user privacy and also inspired some states to enact stronger privacy laws. [55] The EU AI Act will likely have the same effect, prompting meaningful conversations about comprehensive U.S. legislation [56] and resulting in new state laws that cover more themes than they do today.

[46] Orrick, https://ai-law-center.orrick.com/oklahoma/ (2025).

[47] Orrick, https://ai-law-center.orrick.com/mississippi/ (2025).

[48] NY Civ Rights L § 50 (2024).

[49] *Automated Employment Decision Tools (AEDT),* N.Y.C. Admin. Code § 20-870.

[50] Arizona Revised Statutes (A.R.S.) § 20-3103.

[51] Orrick, https://ai-law-center.orrick.com/nebraska/ (2025).

[52] *Florida Digital Bill of* Rights, Florida Statute § 501.705(2)(e).

[53] Montana Consumer Privacy Act, Section 5(1)(e)(iii)

[54] Many of these laws do not refer to automated decision making. Using personal data for "profiling," however, presumes that such profiling is being performed by automated systems, including AI.

[55] *GDPR's Impact on Cybersecurity: A Review Focusing on USA and European Practices,* 11(01) Int'l J. of Sci. and Res. Archive 1340 (2024).

[56] The Center for AI Policy (CAIP) advocates for strong AI legislation and has created a comprehensive model AI Act. More information available at https://www.centeraipolicy.org/category/model-legislation.

# Section 5- Artificial Intelligence Legislation, Governance, and Oversight

## Private and Public Organizational Policies

The release of ChatGPT led to employees across all industries leveraging it and other AI tools for a broad range of purposes. One common use is creating or editing business communication, such as asking a tool to re-write a memo in a different tone, advise on sentence structure, or analyzing a communication for readability. Employees started using generative AI to create graphics, logos, and other visual materials. College students asked AI tools to help write their papers, and secondary school students quickly discovered that AI-driven chatbots could answer their homework questions. Software engineers started asking ChatGPT to review their software code, or even to write it from scratch.

This quick adoption led to early negative outcomes. Two widely reported examples from 2023 are: 1) employees at Samsung who input corporate intellectual property into ChatGPT; [57] and 2) lawyers that asked ChatGPT to write a brief which ended up containing made up ("hallucinated") case law. [58] These two incidents highlight the reasons why policies need to be developed to constrain AI usage in the workplace. After Samsung discovered the data disclosures, they instituted new policies and technological safeguards to prevent additional information loss. [59]

Corporate policies regulating employee behavior are not generally available to the public. Many Higher Education institutions, however, publish their policies on their public websites. Some have policies covering specific employee uses of AI, others include a ban on student usage of AI for their school work in their student code of ethics or handbook, and others provide guidelines in lieu of formal, enforceable policies. [60] A complete review of these policies is out of scope of this paper. Recommendations for provisions that should be included in AI policies include: [61]

- **Governance** – create a governance framework for reviewing and updating the policy and its components based on the progression of AI technology maturity, the evolving legislative and regulatory landscape, and new and innovative use cases. This framework should also include committees and individuals with specified roles and responsibilities in approving AI tools and usage.
- **Define AI** – provide a clear definition of AI in non-technical language so those impacted understand the scope of the policy.

[57] *Samsung Engineers Feed Sensitive Data to ChatGPT, Sparking Workplace AI Warnings,* Dark Reading, https://www.darkreading.com/vulnerabilities-threats/samsung-engineers-sensitive-data-chatgpt-warnings-ai-use-workplace (Apr. 11, 2023).

[58] *Lawyer Used ChatGPT In Court—and Cited Fake Cases. A Judge is Considering Sanctions,* Forbes Business, https://www.forbes.com/sites/mollybohannon/2023/06/08/lawyer-used-chatgpt-in-court-and-cited-fake-cases-a-judge-is-considering-sanctions/ (June 8, 2023).

[59] *Samsung Engineers Feed Sensitive Data to ChatGPT, Sparking Workplace AI Warnings, Dark Reading,* https://www.darkreading.com/vulnerabilities-threats/samsung-engineers-sensitive-data-chatgpt-warnings-ai-use-workplace (Apr. 11, 2023).

[60] A compilation of institutional policies can be found at *Generative AI Policies at the World's Top Universities*, thesify., https://www.thesify.ai/blog/gen-ai-policies-of-the-worlds-top-universities (Feb. 20, 2025). A compilation of institutional guidelines on generative AI usage in the classroom can be found at *List of Institutions with AI Guidelines*, Univ. of LaVerne Wilson Lib., https://laverne.libguides.com/c.php?g=1390420&p=10336863 (last updated Jan. 13, 2025).

[61] Recommendations summarized from *8 Tips for Creating a Comprehensive* "AI in the Workplace" Policy, LexisNexis Legal Insights, https://www.lexisnexis.com/community/insights/legal/b/thought-leadership/posts/8-tips-for-creating-a-comprehensive-ai-in-the-workplace-policy (Feb. 21, 2025).

- **Approved AI platforms** – provide a list of AI tools that are approved for use.
- **Approved use** – provide clear approved uses of AI in the workplace that leverage approved AI tools (eg. drafting business communications).
- **Prohibit disclosure of confidential information** – prohibit the input of individual personally identifiable information or intellectual property into AI tools, unless defined exceptions apply (e.g. permitting such inputs into AI tools that do not retain such data or use it for model training).
- **Human oversight** – require a human to verify the output of AI tools before usage.
- **Preserve intellectual property rights** – define how content created by generative-AI can or cannot be used. Individuals must preserve these right in others, and not use created content based on another's copyrighted work. Similarly, an organization may retain a copyright in all creative works, and integrating AI-generated media may invalidate such copyrights.

### Impact of Legislation and Policy on AI and Cybersecurity Workforce Development

The EU AI Act lays out clear requirements for high-risk AI systems and general-purpose AI models related to cybersecurity, data protection and data privacy. It also requires comprehensive documentation explaining how such systems and models operate, and integrating software or process mechanisms to stop operations (the "kill switch"). Some comprehensive, sectoral, and amended state laws require informed consent, opt-out, human oversight, and mechanisms to prevent discriminatory models. These legislative requirements must be built into the design and development phases of AI systems and models. In addition, private and public businesses have policies that place restrictions on the use of AI, prohibiting the disclosure of business information or leveraging AI to assist in creating work products or educational assignments. This means that individuals educated and trained to create AI systems and models must also be educated in cybersecurity, secure software development, risk management, data privacy, and other practices.

### Recommendations

The following practices should be embedded into AI education courses, curriculums, and certification programs to support current and future AI legislative and regulatory requirements:

1. **Secure Software Development Lifecycle (SSDLC)** – embed cybersecurity, data protection, and data privacy into early and ongoing software development, including 1) security engineering; 2) security assurance; 3) security organizational and project management practices; and 4) security risk identification and management.
2. **Risk Management** – build risk management practices into software development and testing, with repeated practices of identifying, reviewing, mitigating, and accepting risks through formal approval channels. The NIST Artificial Intelligence Risk Management Framework (AI RMF) can be adapted to apply to development activities.
3. **Third-Party Vendor Risk** – understand how AI systems and models may rely on third-party components, and learning how to build software that mitigate risks introduced by using such components.

# Section 5- Artificial Intelligence Legislation, Governance, and Oversight

4. **Technical Documentation** – build expertise in technical documentation and software operating instructions, including creating explanatory language of AI system and model operations for public and private disclosures.
5. **Privacy by Design** – design AI systems and models with a privacy first mindset, building in mechanisms for data anonymization, pseudonymization, blocking personal data from being collected and processed, informed consent, user privacy options, and others. The same principles should be used to add technological controls into AI systems and models to prevent the deliberate and accidental disclosure of trade secrets, copyrighted materials, proprietary business assets, and classified information.
6. **Threat Modeling** – analyze code, systems, and applications for vulnerabilities that could be exploited by attackers and devising ways to eliminate or mitigate them.
7. **Vulnerability and Penetration Testing** – build skillsets in simulating cyber-attacks by actively exploiting vulnerabilities against AI systems and models during development and testing (AI Red Team activities).
8. **Incident Response Tabletops** – design AI specific tabletop exercises to test and validate incident detection and response procedures, processes, and governance.
9. **Human Oversight** – understanding which steps in data collection, processing, and outputs require human intervention by option or requirement, and building such features in early phases of design and development.
10. **Cybersecurity Training** – prospective AI developers, engineers, and others in the AI workforce should have formal training in cybersecurity and privacy best practices. AI certifications should include baseline knowledge of best practices as well.
11. **"Kill Switch"** – build AI systems with one or more technological features that can fully terminate a complex, interconnected system with one action or command by a single operator.
12. **"Closed ecosystem AI development"** which means the practice of developing AI tools specifically for a business so there is zero risk of data loss from business information being exposed by being input into a model.

### Conclusion

European regulations, United States legislation, and AI usage policies in the private and public sector can serve as guides to current and future AI education curriculums. Educators and certificate-issuing bodies like ISACA, ISC2, IAPP, etc. can incorporate the themes highlighted in this paper to better prepare the United States workforce for success in AI system and model design, development, and deployment. Following the recommendations above will also help bring to market AI tools that are purpose-built with cybersecurity, data privacy, and other themes incorporated into their features and functions. This will improve the safety and security of AI tools in the market, reducing the risk of these emerging technologies, and strengthen U.S. National and Economic Security.

# Section 5- Artificial Intelligence Legislation, Governance, and Oversight

**References:**
EU AI Act Explorer – https://artificialintelligenceact.eu/ai-act-explorer/

IAPP United States AI Governance Legislation Tracker – https://iapp.org/resources/article/us-state-ai-governance-legislation-tracker/#state-ai-governance-law-chart

NIST Artificial Intelligence Risk Management Framework 1.0 – https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

NIST Cybersecurity Framework – https://www.nist.gov/cyberframework

NIST Security and Privacy Controls for Information Systems and Organizations (800.53 Rev. 5) – https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Privacy by Design – https://www.aepd.es/guides/guide-to-privacy-by-design.pdf

GDPR Privacy by Design – https://gdpr-info.eu/recitals/no-78/

# Report Conclusions

There are many key themes found within this report. The complexities of the convergence of Cyber-AI has numerous global implications. For purposes of this report, we analyzed and evaluated the impact of Cyber-AI convergence on K-12 Education, Higher Education, workforce development, campus digital infrastructure protection and governance/law, and policy. With significant changes expected in all of these important areas related to professional preparation and workforce development, it is important to understand their origins and evolution. Advice to a security practitioner's AI imperative is a core subject in understanding the value and impact of securing AI on our campuses.

Learning environments are being changed substantially as AI quickly impacts many dimensions of academia. As such, a new generation of legislation, policy, and law are salient and needed today to guide and advise all major partners and key stakeholders. In this report section, we focus on the conclusions of this report and discuss future avenues of research into the following subject areas.

# Report Conclusions

1. The implications for convergence in Cyber-AI must be further evaluated in terms of vulnerability evaluation and risk management. We must remain aware of trends and impacts for both Red Team & Blue Team roles, activities, and operations. We need to ensure that AI is utilized to bolster cybersecurity defenses and enhance organizational and individual privacy and data, and not become a dangerous threat used against organizations, individuals, and our way of life

2. Understand the implications of a converged AI & Security workforce development and education to best protect society, organizations, and individuals. We must better understand connections (i.e. AI and risks, threats, and vulnerabilities) before discussing meaningful program and course curriculum, content, teaching pedagogy, labs, exercises, etc.

3. Design additional education experiences (like professional certifications); and, enhanced workforce experiential opportunities like pre-apprenticeship programs, registered apprenticeship programs, internships, etc.

4. Build a comprehensive Cyber-AI workforce development and education framework (including K-12 and Higher Education) to prepare the next generation of converged AI-enhanced cyber professionals through advanced K-12 and Higher Education programs, courses, and curriculum.

5. Develop and implement a converged Cyber-AI professional preparation framework and structured curriculum that links and aligns these work roles across all stages of the career ladder from entry to executive-levels. A proposed converged Cyber-AI workforce aligned stacking curriculum reference architecture and should be adopted and added to the NIST/ NICE Cybersecurity Workforce Framework 2.0 or future revision. All NICE Cyber workroles are heavily impacted by AI in terms of red and blue team activities.

6. Provide guidance and advice to K-12 and Higher Education Institutions on the effective utilization of AI to protect and defend critical campus infrastructure, networks and technology resources; while maximizing opportunities for collaboration, communication, innovation, and information sharing between faculty, students, and staff.

7. Begin a comprehensive discussion of key governance, policy, and oversight issues as related to Cyber-AI Convergence in the matters of education and workforce development.

This white paper report analyzed and evaluated the transformative evolution arising from the processes of convergence of Cyber-AI education and workforce development and related policy areas. We shall wait for further development and data on the processes and outcomes at work to better understand direct and indirect impacts and implications on workforce development preparation; as well as significantly upgrade societal Cyber-AI knowledge and skills to enhance preparedness/awareness capacities and capabilities. Furthermore, we request future support

# Report Conclusions

and resource allocation for the purpose of upskilling and reskilling within K-12 and Higher Education systems to significantly enhance workforce and campus IT preparation and capabilities for the burgeoning digital environment.

The Cyber-AI policy area is critical for future U.S. economic prosperity and national security in a growing multi-polar world of conflict and strained relations with geopolitical adversaries. We must develop a comprehensive, scalable, feasible, and practical national Cyber-AI education and workforce development strategy to maintain a strategic edge and comparative advantage to counter and constrain a growing bold group of adversarial nations that seek to use security and AI vulnerabilities to our disadvantage.

Towards this objective, we developed a series of important policy, technical, and structured workforce curriculum to meet these growing international challenges head on. As a group of SMEs in cybersecurity and AI Education and Workforce Development, we hope that readers find this information meaningful and a good place to start as our educational and workforce needs continue to change at this current rapid rate of emerging technologies such as cyber and AI. In addition, it is our sincere hope that this report and its contents will assist American policy- and decision-makers in these early and transformative days of the AI era.