



# AI Impacts on Cyber Security Workforces

## in the US, UK and Australia

A draft background paper released for comment

26 May 2026

©Social Cyber Institute, CSE Connect and NCyTE 2026

under Creative Commons license



Contacts: [greg.austin@socialcyber.co](mailto:greg.austin@socialcyber.co); [nigel@cseconnect.org](mailto:nigel@cseconnect.org); [costis.toregas@gmail.com](mailto:costis.toregas@gmail.com)

**Abstract:** This paper examines the impact of artificial intelligence on cyber security workforces in the United States, the United Kingdom and Australia. It advances a matrix approach to the classic levels of analysis schema (international system, the state, the sub-national and the individual) rather than treating any of the four as single levels. It prefers a multi-dimensional grid in which any of the levels, and elements within them, can interact directly and simultaneously. This departure is necessitated by the empirical reality that the most consequential dynamics shaping AI cyber workforces in all three countries bypass conventional levels of analysis approaches. Central to this multi-dimensional matrix approach is the inescapable pre-eminence of the US in the political economy of AI cyber: not simply as a state actor that disposes superior investment capacity, but as the dominant site of private-sector decisions (by Microsoft, Google, Anthropic and OpenAI) that define the global threat landscape, the global defensive toolset, and the global supply of AI cyber talent. The UK and Australia appear less as partners of the US than as downstream recipients of technology trajectories and workforce pressures whose terms are substantially set elsewhere. Three scenarios (conservative, moderate and radical) frame the analysis of workforce reform across all three countries. Current evidence places all three in the conservative to early-moderate band. The paper suggests that a structural lag between AI adoption and workforce preparation may be universal and that AI sub-field distinctions will likely remain underdeveloped in national workforce frameworks. The educational organisations in this project may be better positioned to drive reform at the sub-national level than to wait for national strategies to stabilise and align or for the pace of international AI development to slow.

**Keywords:** artificial intelligence, cyber security, workforce development, levels of analysis, political economy, United States, United Kingdom, Australia

## Executive Summary

Assessing the impact of artificial intelligence (AI) on cyber security workforces is in its early stages globally. Data availability is a major challenge along with the potential pace of change and the high complexity of AI technologies. There is strong evidence that pre-existing concepts of cyber security workforces need to be examined before we can analyse the changes. The paper does that. It then addresses the workforces in the United States, the United Kingdom and Australia. This is a discussion paper with provisional findings. It will form the foundation for subsequent analysis of the impacts on education and training in the three countries. The paper is part of a trilateral collaboration of the Australia-based Social Cyber Institute, CSE Connect (UK) and NCyTE (US) that includes a series of workshops running from June to September 2026. We use the term “AI cyber” as the emerging fields of AI-enabled cyber security and AI-degraded cyber security.

**Context and urgency.** AI affects cyber security on two intersecting vectors. The first is technical: AI can dramatically alter the practices, efficacy and economics of both attack and defence through automation, speed, scale and deception. The second vector is socio-political: AI can disrupt pre-existing power and social relationships at every level from the global to the individual. These two vectors intersect and on one view are inseparable. The management of the AI effects is, as NIST observes, more contextual, dynamic and opaque than conventional cyber security risk, and harder to predict, diagnose and document. Against this background, workforce planning for AI-enabled cyber security in 2026 remains highly speculative, even as the pace of change accelerates. One implication of this paper is the risk that evolving workforce strategies and education programmes will be overtaken in their relevance by the AI revolution before adequate reforms are in place.

**Analytical framework.** We use a matrix approach (multi-dimensional) that builds on the framework of Hollis and Smith (1991) for levels of analysis in international relations. Hollis and Smith identify four levels of analysis in a hierarchy (international, national, sub-national and individual) which create debates between adjacent levels but not with non-adjacent levels). Rather than examining each debate pair in sequence (international system against state, state against sub-national, sub-national against individual), the paper treats the levels as a multi-dimensional grid in which any combination of levels may interact simultaneously and in either direction. This allows for more debate configurations than the original Hollis and Smith framework provides for.

The paper calls out the need to analyse AI cyber impacts with some granularity according to the sub-fields of AI, such as machine learning (ML), large language models (LLM), deep neural networks (DNN), generative AI (Gen AI) and computer vision.

**Three scenarios.** Because comprehensive data is scarce and the future political economy of AI is highly uncertain, the paper develops three scenarios for AI cyber workforce development. The conservative scenario is one where AI reform is viewed as incremental and where there is a low appetite for reform among the most powerful stakeholders. The moderate scenario involves pockets of rapid workforce reform and an increasing appetite for it. The radical scenario is one where AI agents operate autonomously, human roles shift largely to governance and oversight and there is a high appetite for corresponding workforce reform. Current evidence places our three subject countries in the conservative to early-moderate band. At the same time, the pace of change between 2024 and 2026, particularly in agentic AI and adversarial capability development, suggests the window available for conservative and moderate reform may be shorter than stakeholders assume. Pressure across the matrix may be running ahead of the institutional responses available at any single level.

**Country findings.** The US leads in both AI cyber investment and in articulating competency frameworks for a reformed AI cyber workforce based on sub-fields. It has not yet implemented the structural workforce transformation that the National Security Commission on Artificial Intelligence judged necessary in 2021. A US\$6 billion federal and state investment in AI workforce development since 2023 has been assessed by one observer as structurally inadequate ("a gesture not a strategy"). The UK has set up the most systematic national data set on AI use and training within the cyber workforce. It has establishing useful measurement baselines for the workforce settings. Yet its statistics are somewhat elementary. The UK has been slow to treat AI as a single workforce category and in distinguishing the sub-fields (machine learning, adversarial ML, generative AI, agentic AI) that require distinct skill sets for cyber security. The rapid growth of UK-based firms offering cyber security for AI systems, from 66 in early 2025 to 111 by 2026, illustrates the pace of commercial development relative to the slower pace of workforce planning. Australia has high-level digital and AI strategies, particularly in the public sector. It has yet to develop AI-specific cyber workforce architectures or to reflect AI sub-field distinctions in national role taxonomies, though the federal civil service is moving on that direction.

**Cross-cutting findings.** Across all three countries, the dominant finding is a structural lag between AI adoption and workforce preparation. Most cyber professionals are using AI tools without formal training and without observing principles of responsible AI. Early-career roles are being compressed faster than new pathways are created. The sub-field distinctions that matter most for effective AI cyber work are not consistently reflected in educational programme design or national qualifications frameworks. The SANS Institute's assessment that the crisis is not a talent shortage but a skills production problem captures the central challenge with precision.

**Implications for the sponsoring organisations.** The educational community represented by the Social Cyber Institute, CSE Connect and NCyTE may have an opportunity to influence national strategies of AI cyber workforce reform. They may however be better positioned to work on sub-national reform. The workshops following this paper should engage directly with AI sub-fields, with scenario-based competency design, and with the institutional and faculty change required to sustain relevance in a period of accelerating transformation. Preparing educators and stakeholders in education policy to anticipate trends would constitute a strategic contribution. A strong input for arriving at impactful and adoptable solutions is the engagement of government and industry voices to the subsequent phases of these workshops.

## Contents

|                                                  |    |
|--------------------------------------------------|----|
| Executive Summary                                | i  |
| Introduction                                     | 1  |
| Context and uncertainty                          | 2  |
| What is the workforce for AI cyber?              | 2  |
| AI sub-fields                                    | 4  |
| Data deficit for AI cyber workforce reform       | 5  |
| Choices for AI cyber workforce reform            | 6  |
| Scenarios for AI cyber workforce reform          | 7  |
| Political economy of AI cyber                    | 9  |
| Workforce reform for AI cyber in the US          | 10 |
| <i>Role changes at the coalface in the US</i>    | 14 |
| Workforce reform for AI cyber in the UK          | 16 |
| <i>Role changes at the coalface in the UK</i>    | 18 |
| Workforce reform for AI cyber in Australia       | 19 |
| <i>Role changes at the coalface in Australia</i> | 20 |
| Trilateral comparisons                           | 22 |
| Conclusion                                       | 23 |
| References                                       | 24 |

## Introduction

In early 2026, the Social Cyber Institute, based in Canberra, in dialogue with the UK 's CSE Connect and US organisation, NCyTE, agreed to embark upon a tripartite investigation of the impact of artificial intelligence on the cyber security workforce as its increasingly responds to the security consequences of AI-enabled environments . This paper describes this field of activity as "AI Cyber" through this paper. The investigation has the aim of understanding its impact primarily on education, and therefore the preparation of people to participate in current and future workforce. The investigation includes three online workshops during the period June to September 2026, supported by various independent initiatives and events already planned, such as CSE Connect Annual Conference in Dundee, Scotland in July 2026.

This version of the paper is written specifically to support the first online workshop on 2<sup>nd</sup> June, hosted by the Social Cyber Institute. This workshop aims to examine the assumptions, scenarios and trends in demand for AI cyber workforce reform. Subsequent workshops will dive deeper into competencies required in relation to the scenarios. A final workshop will focus on institutional and faculty change at a time of technological revolution.

As a question of educational practice in cyber security, the aims of this investigation are driven by the high degree of uncertainty regarding future roles, skills and knowledge required in the workforce, and the potential speed, scale and scope of change. There is a risk that the requirements driving current educational programmes may be overtaken in terms of their relevance by the speed and scope of the AI revolution. Educators, and indeed employers, therefore, have no choice but to hedge this risk by trying to estimate what future skills and roles may be needed.

There are different approaches to the concept of cyber security. For example, ITU work suggests a heavy focus on protecting the cyber physical environment, its organisation and assets. The World Economic Forum sees technical protection of systems as only part of the task and encourages leaders to manage social impacts and consequences, such as polarisation, erosion of public trust, privacy concerns and ethics. Oxford University's Cybersecurity Capacity Maturity Model (CMM) organises cyber security across five dimensions: policy and strategy, culture and society, education and training, legal and regulatory frameworks, and standards and technologies. Education programmes in cyber security around the world address this spectrum of interpretations without forcing a clear choice.

This paper is not a general survey of the AI workforce. Its core concern is narrower: the effect of AI on cyber security workforces. Broader developments in the general AI labour market are discussed only where they materially shape AI cyber capability through investment patterns, immigration settings, university capacity, or enterprise adoption. This distinction matters because generic claims about "AI skills" can obscure the specific technical, governance, and assurance capabilities required in AI cyber roles.

It should also be noted that the approach does not look at non-English speaking efforts beyond the three countries addressed. For example, the UAE's Falcon ecosystem is supported by a new university to build Arabic-language AI capabilities, to foster AI-based economic development and to position Abu Dhabi as a hub for the international AI community. (Mohamed bin Zayed University of Artificial Intelligence). China and Japan have large-scale national programs to expand domestic AI talent and infrastructure. Future iterations of this project on AI cyber workforces beyond 2026 could extend the framework to incorporate a more explicitly global comparison of AI workforce and capability strategies.

This paper is a comparative scoping study rather than a causal test of specific interventions. It draws primarily on recent government reports, professional surveys, industry analyses, labour-market commentary and selected academic literature.

The analysis proceeds in three stages. First, it maps the problem using an expanded levels-of-analysis framework derived from Hollis and Smith (1991), supplemented by later agent-structure scholarship. Second, it distinguishes relevant AI sub-fields because the workforce implications of machine learning, generative AI, adversarial machine learning, agentic AI, and trustworthy AI are not identical. Third, it uses exploratory scenarios to organise comparison across countries under conditions of severe data scarcity.

The paper does not claim cross-national measurement equivalence. The available evidence differs significantly across the three countries in depth, definition, and periodicity. Accordingly, the comparison is interpretive and policy-oriented. The aim is to identify patterns, asymmetries, and strategic gaps rather than to produce a harmonised relative ranking.

## Context and uncertainty

Tools employing artificial intelligence (AI) affect cyber security on two main vectors. The first is the technical vector where they dramatically alter the efficacy and economics of attack or defence (through reliance on scale, speed, precision, deception and/or automation). The second vector is socio-political where their use significantly disrupts pre-existing power and transactional relationships at many different levels from the global to the individual. The second vector includes the question of AI governance, but that is only a very small part of the social, economic and political impacts of AI on cyber security.

The ways in which these two vectors intersect in any specific instance of AI use are highly diverse, but for a single point in time they are often observable and intelligible. It is tempting, therefore, to assume that at any given moment these intersections are manageable. However, the history of such intersections (past configurations and consequences) is effectively unbounded and cannot be fully apprehended by any individual decision-maker, or even a highly capable group.

More simply put, and as summarised by a leading US agency, in a security context, “AI behaviour and vulnerabilities tend to be more contextual, dynamic, opaque, and harder to predict [than for non-AI cyber security], as well as more difficult to identify, verify, diagnose, and document, when they appear” (NIST 2025, 10) . The management of such issues, even when they can be identified, is a highly demanding task since “some vulnerabilities are inherent to the AI model or the underlying training data and machine-learning infrastructure”. Moreover, Microsoft’s reporting that it oversees “ billions of users, millions of organizations” and records trillions of “security signals” each day (Microsoft 2025, 6).

In 2026, these considerations of scope mean that workforce planning in response to AI impacts on cyber security remains highly speculative and experimental even as organisations like NIST and Microsoft look for comfort and pre-existing approaches to risk management approaches borrowed from cyber security.

## What is the workforce for AI cyber?

In its simplest terms, “workforce” means a group of people who work in a specific enterprise, sector, geographic locality, country or multinational environment. In common usage, this also can include not just present workers but those who had worked in those places or might do in the future. Thus, there are at least four levels of analysis potentially in

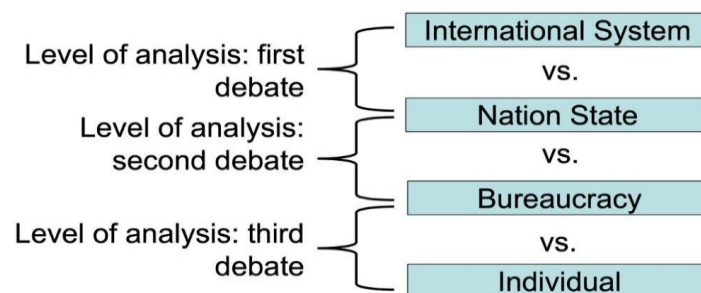
play: individual, sub-national, national and international. To this framework, we could add regional and even sectoral levels operating across the four levels. We could for example include the perspective of multi-national and non-state actors. Individuals of interest are diverse and in the context of workforce include researchers, officials, business leaders, workers and lawyers amongst many others. Sub-national actors include businesses, professional bodies, legislative bodies, and members of civil society and so on. Trends over time are also central to the analysis.

Treating each level separately has genuine value for mapping the problem space. It makes visible the very different kinds of claims being advanced at each level. On the other hand, beginning this research, it is immediately clear that research on the AI cyber workforce does not fit neatly within the boundaries of any single level of analysis. Its development is driven by sub-national and trans-national actors, shaped by state policy, constrained or enabled by international arrangements, and ultimately expressed through the decisions of individuals. Examined in isolation, the focus on a single level produces an incomplete and potentially distorted picture. International analysis risks obscuring the domestic political struggles that shape national AI cyber strategies. Individual-level analysis risks overstating the autonomy of human decision-makers in systems where the choices available to them maybe largely predetermined.

We prefer to use a matrix approach (multi-dimensional) that builds on the framework of Hollis and Smith (1991) but goes beyond it.

Hollis and Smith chose not to treat the levels of analysis as self-contained alternatives, but rather to organise them as a series of nested debates, each forcing a methodological choice about the relationship between structure and agency across levels. This is illustrated in Figure 1.

**Figure 1: Intertwined Levels of Analysis (Hollis and Smith 1991)**



The four levels we identified interact with others. Hollis and Smith represented this interaction as a set of three debates. In each debate, one can consider the top level to be a system, and the lower level to be a unit. In addressing an issue, one can proceed top-down or bottom up, each approach offering an insight into the dynamics at play. For example, at the First level of debate between nation state and international system, we can see how the United States’ Presidential delegation to China in May 2026, consisted of officials and CEOs of technology enterprises. Seen as a State, the US was applying its prowess and power in technology to influence the international system through its interaction with other nation states engaged in systematic competition. At the second level of debate, one can observe bureaucracies and enterprises, in this case the individual tech companies, interact with the national government by setting up a new system of relationships and ways of working under the leadership of President Trump. Whilst this has some explanatory power in terms of the dynamics in relationships, one should not forget that individual actors in what Hollis and Smith call the “bureaucracy” (such as Google) also have

significant power over international systems, and indeed the behaviour of individuals. The levels are clearly identifiable but are porous and complex in terms of their interaction.

Rather than examining each debate pair in sequence (international system against state, state against bureaucracy, bureaucracy against individual), the paper treats the levels as a multi-dimensional grid in which any combination of levels may interact simultaneously and in either direction (Wendt 1993, Wight 2006). This allows for more debate configurations than the original Hollis and Smith framework provides for. For example, we can consider the direct interaction between individual AI developers and the international regulatory system, potentially bypassing the state entirely, or the way in which enterprise-level AI adoption decisions feed back upward to reshape national workforce strategy rather than simply receiving it.

As a further example, consider the international and local systems for the demand and supply of skills, through influences like capital accumulation, labour quality, immigration policy, productivity and economic trends. With these considerations in mind, nationality descriptors for a given workforce will need to be carefully deployed in the light of three important factors: the availability of international or regional migration, the option for remote working (“work from home”) in foreign countries, developed during the Covid pandemic, and the use of foreign-based subsidiaries or contractors. It is not common practice for corporations to reveal these sorts of details about their workforces. Governments provide some data but it is usually fragmentary and not longitudinal. A bottom up versus a top-down reading of the skills demand and supply system reveal a multiplicity of dynamics at work. This allows us to explore how the actions of individuals as agents influence a system, as well as systemic influence on the actions of individuals.

## AI sub-fields

Our analysis pays some attention to the consideration that AI as a technology category has many subfields which present distinct challenges in analysing its impact (Social Cyber Institute 2025: 25): “The more established subfields include machine learning (ML), computer vision, and natural language processing (NLP). Emerging subfields include reinforcement learning (RL), generative AI, and self-supervised learning. Frontier sub-fields include cutting-edge innovations such as neuromorphic computing (brain-inspired hardware) and federated AI (decentralized learning). AI applications often rely on the integration of several of these subfields”. Table 1 offers an analysis of how these sub-fields are influential in cyber security based on the NIST and Microsoft reports referenced above.

**Table 1: Impacts of AI on Cyber Security (NIST 2025, Microsoft 2025)**

| <b>AI sub-field</b>                                 | <b>Impacts on cyber security</b>                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Generative AI and large language models             | Most immediate impact: phishing, spear-phishing, malware assistance, reconnaissance, social engineering, disinformation, automated reporting, and cyber training. Microsoft says threat actors are using AI to scale phishing and automate intrusions, while defenders use AI for analytics, phishing detection, remediation, and incident response agents. |
| Machine learning for detection and anomaly analysis | Core to modern cyber defence: endpoint detection, network anomaly detection, user/entity behaviour analytics, fraud detection, identity-risk scoring, SIEM/XDR alert triage, and cloud monitoring. NIST frames “AI-enabled cyber defense” as one of the three central AI cyber focus areas, alongside securing AI systems and thwarting AI-enabled attacks. |

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Agentic AI and autonomous planning                      | Potentially transformative because it moves from “AI as assistant” to “AI as actor”: automated vulnerability discovery, attack-chain orchestration, SOC triage, incident containment, ticketing, patch prioritisation, and adaptive response. Microsoft notes that AI agents can act within seconds, for example suspending compromised accounts and triggering password resets when high-risk signals align.                                                                                |
| AI for software engineering and vulnerability discovery | High impact because cyberspace is software-dependent: AI can help write code, find bugs, generate tests, fuzz systems, assist exploit development, review infrastructure-as-code, and secure or compromise software supply chains. Microsoft reports that adversaries are using generative AI for automating lateral movement, discovering vulnerabilities, and evading security controls, while defenders must shift from static detection toward behaviour-based and anticipatory defence. |
| Adversarial machine learning and AI security            | Crucial because AI systems themselves are now attack surfaces: prompt injection, data poisoning, model manipulation, model theft, training-data compromise, inference attacks, and malicious tool-use by AI agents. NIST’s Cyber AI Profile explicitly separates “securing AI systems” from “AI-enabled cyber defense” and “thwarting AI-enabled cyberattacks,” which is a useful policy taxonomy.                                                                                           |
| Privacy-preserving AI and trustworthy AI                | Vital for safe deployment: federated learning, differential privacy, secure enclaves, model governance, data provenance, evaluation, auditability, and privacy-preserving analytics. CISA-linked guidance has emphasised AI data-security risks including data supply-chain risks, maliciously modified data, and data drift                                                                                                                                                                 |

From the perspective of job roles, the differences in these sub-categories are sufficient to suggest that we complement generalised commentary applicable to all types of AI, with some consideration of how different sub-fields might affect the workforce picture. For example, though in the table 'privacy-preserving AI and trustworthy AI' as a separate row above, its importance is paramount from a risk perspective across all other AI domains. Secondly, AI as an 'alarm' in threat discovery, is materially different from AI as an agent. There is a question of what is delegated to the AI tool where a human would normally make a judgement (for example, when to escalate). Workforce planning must differentiate between AI that just assists analysts and AI that actually takes over parts of their judgement. This distinction is central to the paper’s purposes: a workforce strategy that treats AI as a single undifferentiated capability would risk over-simplification of both future roles and future training needs.

A multinational report on AI cyber in 2024 supported by 11 countries including the Five Eyes called out the distinction between sub-fields of AI and gave examples of how they are used (ASCSC 2024). Microsoft (2024) issued a similar primer. A literature review from 2024 indicates research trends for AI cyber. It concludes that “deep learning (DLs) models such as convolutional neural networks<sup>1</sup> and recurrent neural networks are the most adopted method because of their high performance in extracting hierarchical features from high-dimensional data “ (Ashfin 2024: 22). That analysis reported that after 2020 there was a shift to the development of “explainable and federated models: and a focus on transparency, accountability, and privacy-preserving learning”.

### Data deficit for AI cyber workforce reform

There are severe limitations on public knowledge of AI cyber workforce development for all levels of analysis and debates (individual, enterprise, national, and international). These

---

<sup>1</sup> According to IBM, convolutional neural networks (CNNs) are a type of deep neural network that are especially good at recognising patterns in data with a grid-like structure, such as images, video frames, or some kinds of time-series and signal data.

deficits are particularly more visible for the private sector than for the public sector. Few governments have yet organised comprehensive data collection on AI cyber. Though there is limited evidence of engagement and consultation with stakeholder groups on fairly broad issues (Wetzel 2025).

Even the best surveys appear to stop at addressing AI adoption sentiment and views of productivity in cyber security. They do not analyse sub-category fields, roles and competencies for AI cyber. A SANS study on cyber security workforce based on a global survey of 947 (self-selected) respondents begins to open up useful but still limited data sources (SANS GIAC 2025).<sup>2</sup> The study cites a leading industry figure: “The industry hasn’t invested yet in giving management the tools to understand what developing people means in an AI-enabled world’ (p. 6).<sup>3</sup>

A key problem is not simply lack of data, but lack of commensurable data. Surveys often measure AI adoption sentiment, productivity expectations, or general digital capability, while leaving under-specified the sub-fields of AI involved, the cyber roles affected, and the depth of training provided. This limits robust cross-national comparison and helps explain why workforce planning remains broad-brush in all three countries.

## Choices for AI cyber workforce reform

Data requirements will change depending on the choices made by policy makers and planners about a number of enduring structural choices or influences that shape the cyber security sector. A set of these was presented after a trilateral collaborative project on cyber security education conducted at the University of New South Wales Canberra between 2017 and 2019 (Austin 2020: 209). These are all highly consequential for current planning in workforce development for AI cyber. With some amendment for an AI focus, they are listed below.

- What sort of information society do we want: balancing AI threat and opportunity
- What sort of security do we want in cyberspace: how do we balance freedoms against technological pressures and wealth creating potential
- Establishing the evidence base for national and sub-national skills policy for AI cyber
- Education policy choice points beyond curricula for AI cyber
- Promoting maturity in education systems for AI cyber
- Focusing on resilience and dependency for AI cyber (a missing link in education and training)
- Managing offshore workforces for AI cyber
- Cost transfer for training and skills between the globalised private sector and nationally-focussed public sectors for AI cyber
- Online education (international and domestic) for AI cyber
- Managing new disruptive technologies in AI cyber
- Formal knowledge versus self-taught informal knowledge for AI cyber
- Critical thinking, personal resilience and individual ethics as the core abilities of AI cyber workforces.

---

<sup>2</sup> The survey was based on 947 global respondents across six regions: North America (56 per cent), Europe (16 per cent), Latin America (14 per cent), Asia-Pacific (7 per cent), Africa (5 per cent), and the Middle East (2 per cent). Respondents represent cyber security/InfoSec leadership (72 per cent), HR/talent acquisition professionals (16 per cent), and those with both responsibilities (12 per cent). Organisations span small businesses to enterprises with more than 100,000 employees across more than 20 industry sectors.”

<sup>3</sup> The SANS report is citing Jay Bhalodia, Rebuilding the Pipeline: How Microsoft Balances AI Acceleration with Workforce Development, which is a short case study in the SANS report.

## Scenarios for AI cyber workforce reform

For the reasons cited above, but especially the lack of reliable data, the paper proposes three scenarios to try to assess the emerging situation of AI impacts on the cyber security workforces of any country. The scenarios can be summarised as follows:

1. Conservative – a low appetite for reform of the workforce and the labour market
2. Moderate – a variable appetite for reform of the workforce and labour market
3. Radical – a high appetite for reform of the workforce and labour market.

The characteristics of these scenarios are based on two plausible assumptions:

1. The work context will move broadly from people-centric tasks assisted by AI to AI agents supervised by people
2. Business models will transform from those we recognise today to business models that enable an AI first architecture.

Note the development of the work context, business model and regulatory environment for the three scenarios below were developed with the assistance of Google Gemini by prompting with the two assumptions above and then edited by the authors.

### **Scenario 1: Conservative (Low appetite for workforce and labour market reform)**

- Work Context (Assumption 1): AI remains largely an assistant. People do the heavy lifting. "AI Agents" are restricted to low-risk usage. Job roles remain relatively stable.
- Business Models (Assumption 2): Traditional in-house security functions and MSSP (Managed Security Service Provider) models endure. Pricing is still tied to headcount, data volume or licenses.
- Regulatory Environment: Although slow to be implemented, government regulations will mandate human oversight for compliance. Insurance companies will need evidence of human control.

### **Scenario 2: Moderate (Variable appetite for workforce and labour market reform)**

- Work Context (Assumption 1): A "hybrid co-pilot" reality. High-maturity/ wealthy organisations move to human-supervised AI agents for standard incident response (e.g., automated containment of ransomware). Less mature/ wealthy industries stick to assistant-level AI due to budget or skill gaps. Job roles change with more supervision of AI agents, reduction in traditional deep tech knowledge and skills associated with today's cyber security. Core business and communications skills become a differentiator in the job market for roles at mid-level. Early career roles under pressure.
- Business Models (Assumption 2): Transitional business models emerge at varying speeds, focusing some companies out of business. We see the rise of "Outcome-Based Pricing" where security vendors charge based on SLA resolution times.
- Regulatory Environment: Regulations are outcome-focused rather than process-focused.

### **Scenario 3: Radical (High appetite for workforce and labour market reform)**

This is an "AI-First" paradigm.

- Work Context (Assumption 1): Fully autonomous AI multi-agent swarms. The human role shifts entirely from *operational* to *governance*. Humans do not monitor

alerts; they monitor the AI's reward functions, define high-level security policies, and audit the system's decisions post-incident.

- Business Models (Assumption 2): Total disruption. Security is built natively into the "AI-first" architecture of enterprise applications. Traditional perimeter security and standalone SOC's (Security Operations Centres) disappear, replaced by self-healing, decentralized code environments.
- Regulatory Environment: Liability frameworks have evolved to treat AI agents similarly to legal corporate entities or auto-pilot systems, where software manufacturers or certification bodies hold the liability, freeing enterprises to automate aggressively.

For all three scenarios, we can consider a range of indicators that help inform the debates in the level of analysis problem discussed earlier. These include, but are not limited to:

- Mapping AI-specific competencies (sub-fields) for security
- Assessing productivity/effectiveness of specific AI tools
- AI skills mapping
- Role redesign for AI
- AI governance process
- AI-augmented workflows
- Automation adoption rate
- AI security specialisation
- How well nested are AI-specific competencies in an over-arching framework for a workforce of digital workers where AI is one of a number of key competencies
- Continuous education and training programs
- Talent impact evaluation

The first implication is that collective action by any combination of the actors to meet a single indicator for a separate level of analysis would likely provide an instant efficiency dividend. A second implication is that to assess AI cyber workforce development in a single country such as the US, the UK and Australia is far from a simple exercise. In the absence of comprehensive data, the analysis should be read as a comparative scoping exercise: evidence-based, but necessarily interpretive, and intended to support further empirical research rather than to close debate.

The state of play of AI use globally or in various localities will potentially be a principal driver of which scenario for workforce and education reform emerges in a particular country. One element of the state of play will be the threat environment. In theory we might imagine that we could craft scenarios for the threat environment that match the three scenarios for reform and act as a driver:

- Scenario 1 Threat Landscape: Attackers use AI to scale up traditional attacks (better phishing, faster vulnerability scanning and defensive teams try to defend using legacy tools with basic AI features).
- Scenario 2 Threat Landscape: Adversaries deploy fully automated AI-enabled malware that mutates in real-time. This forces organisations to adopt autonomous tools, because human reaction times are too slow. This puts pressure on the human in the loop thesis.
- Scenario 3 Threat Landscape: "Machine vs. Machine" warfare. Cyberattacks happen at microsecond speeds. A human-centric defence in this scenario is entirely obsolete; only autonomous AI can counter autonomous AI threats.

There is however room to argue that the cyber policies of the majority of states react only slowly to system level threats in cyberspace.

## Political economy of AI cyber

One departure point of this analysis is the reality that the US private sector is the current pace setter on the global scene both in AI and cyber security services. When it comes to government capability, the US is the single most capable country in AI-enabled cyber security, and in this it is supported substantially by the UK and Israel though these are far from being close to the US in AI capability and potential. The single country with most impact on the global education and skills ecosystem for AI-enabled cyber security is also the US. This judgement is based on QS and the Times Higher Education rankings of US universities relative to other countries,<sup>4</sup> data in the Stanford AI Index (2025), and data in the Fortune 500 of the wealthiest global ICT and telecommunications corporations [source this for 2026].

This broader political economy matters to AI cyber because national workforce systems do not operate in isolation. University capacity, enterprise demand, immigration flows, cloud concentration, and the global market power of major technology firms all shape what kinds of cyber capability can realistically be developed domestically, and at what speed.

A quick proxy test of the relative balance is to look at which countries have companies that are household names in the global cyber security sector and which do not, and to compare the footprints of Chinese cyber security companies in the biggest global markets for cyber security services, which are the US, Europe and East Asia (China, Japan, South Korea and Taiwan). G7 countries actively work to constrain the expansion of Chinese ICT and AI capabilities, especially when it comes to security aspects. The US corporations, most with highly globalised workforces, clearly dominate this field in economic power and technical capability and this influences workforce development for AI impacts on cyber security. This leadership position of the US includes capability for defence against AI-enabled cyber threats from China or Russia.

A detailed study of the cyber security sector in the UK in 2025 further demonstrates this dominating reality. In the UK firms that specialise in cyber security for AI, those that are headquartered in the UK represented 48 per cent of the count, while those headquartered in the US represented 38 per cent of the count (DSIT 2025a). The other 14 per cent were based in the European Union or elsewhere. Those with UK headquarters included Tessian, Darktrace, and Mimecast, while those with US headquarters included Checkmarx, Rapid7, Anomali, CrowdStrike and Palo Alto Networks. A 2026 UK government report notes the balance between large firms with UK headquarters in different terms. It says “153 large firms are UK headquartered with estimated UK cyber security revenue of £6.1 billion”, while 87 large firms headquartered outside of the UK produced an estimated “UK cyber security revenue of approximately £4.2 billion” (DSIT 2026). The 2026 report shows a slight shift in the US share of UK-based AI cyber companies headquartered in the US: 47 per cent of firms with UK headquarters and 40 per cent of firms headquartered in the US.

This context shapes how all countries, including the US, UK and Australia must manage their workforce development for AI-enabled cyber security. The concept of ‘sovereign AI’ capability is a politically useful term that captures the necessary aspirations of many countries to deal with workforce issues around AI in general, but for the most part AI-enabled cyber security capability around the world is shaped by industry and governmental trends in the US or in US-dominated global enterprises. Only a narrow slice of any other

---

<sup>4</sup> Of considerable note, India is becoming an influential source of talent in one sub-sector of AI-enabled cyber security and that is platform engineering. In comparison, neither China nor Japan make the same contribution as India from their domestically-based workers to the global workforces for AI-enabled cyber security.

country's AI-enabled cyber security could be regarded as being 'sovereign'. The bigger part of this narrow AI sovereignty slice in the cases of the UK and Australia relates to signals intelligence, national security command and control, and weapons systems, though these are highly integrated with US government systems and rely on technology of US origin.

## Workforce reform for AI cyber in the US

The US case is especially important not because general AI workforce trends can be equated with AI cyber, but because US investment levels, university capacity, platform firms, and federal strategy shape the global conditions within which AI cyber workforce development occurs.

To understand the challenge of workforce development for AI cyber in the US, the best single source may be the 2021 report of the National Security Commission on Artificial Intelligence (NSCAI 2021). This commission comprised a highly authoritative mix of stakeholders (industry, government and research). Its primary focus was the AI workforce, understood as the enabler of all AI capabilities. Its focus is not AI impacts on cyber security but AI in general.

The NSCAI cites research from a highly credible think tank at Georgetown University that the "majority of workers in AI-related jobs and students in AI-related graduate programs are not originally from the United States" (Zwetsloot, Heston and Arnold 2019). This positions any analysis of workforce issues at the outset, even for the US, as a matter of international political economy, diplomacy and immigration policy, as elaborated later.

What therefore does the Commission recommend for development of the US AI workforce? It takes a radical position: the establishment of an AI corps. The implication is that without such radical reform, the US cannot retain its position of dominance in global AI capability which was an explicit part of the Commission's terms of reference. The tone is clear and sharp:

We should establish a new Digital Service Academy and civilian National Reserve to grow tech talent with the same seriousness of purpose that we grow military officers. The digital age demands a digital corps. (p. 3)

The report noted the urgency of such action: "The talent deficit in DoD and the IC [intelligence community] represents the greatest impediment to being AI-ready by 2025" (p.10). The threat was seen as imminent and the report warned against a conservative response:

"For the first time in our lifetime, the United States risks losing the competition for talent on the scientific frontiers. The United States needs to invest in all AI talent pipelines in order to remain at the forefront of AI now and into the future. A passive strategy will not work in the face of the AI talent competition" (p. 173).

Aggressive international recruitment was needed:

"The United States risks losing the global competition for scarce AI expertise if it does not cultivate more potential talent at home and recruit and retain more existing talent from abroad. The United States must move aggressively on both fronts. Congress should pass a National Defense Education Act II" (p. 11).

In terms of the levels of analysis debates, the NSCAI work is firmly placed in the first debate between the nation and the international system. That is, the emerging competition internationally has called for a national response.

Since the NSCAI Final Report in 2021, the US has moved selectively in the direction the Commission urged but its response has so far been insufficient to close the AI talent gap. Federal initiatives, such as America's AI Action Plan (2025) released by the White House, commit to expanding AI programme enrolment, investing in AI teaching capacity, and easing immigration pathways for highly-skilled AI workers. A 2025 report estimated that the U.S. still faces a shortage of more than 4 million AI-related workers, with around 36 per cent of AI roles unfilled (Comrise 2025). These numerical estimates might be challenged on various grounds but other assessments reach similar conclusions. Bain & Company (2025) finds that AI talent remains "scarce" and is expected to be a binding constraint through at least 2027. A 2025 employer survey reported that 79 per cent of U.S. workers feel unprepared to use AI at work, even as adoption accelerates (Bright Horizons 2025). A 2026 audit of federal and state AI-workforce programmes estimates roughly US\$6 billion in federal and state funding since 2023 but concludes that this response is "structurally inadequate," a "gesture not a strategy", similar to "sending a garden hose to fight a wildfire" (AI Exposure Institute 2025). This source argued that meaningful change would require ten to twenty times more effort. There is room to conclude that a skills shortage in AI cyber is the result of a production problem. This will be the subject of subsequent work in this project.

There isn't a standalone "2026 AI talent report" from the White House equivalent to the 2025 AI workforce documents from the Administration. It folded the AI-talent issue into broader 2026 policy packages. One of these, a four-page document, includes a brief Workforce and Education section, calling for "educating Americans and developing an AI-ready workforce," integrating AI training into existing education and workforce programs, and expanding federal research on AI-driven labour-market impacts. The Administration pivoted toward a state-led effort, while reserving its policy attention to fighting or overturning state legislation that ran against Administration policies of minimalist regulation, as captured in Executive Order 4365 of December 2025 (White House 2025).

Thus, the US government has not yet implemented the kind of large-scale "AI corps" architecture that the Commission viewed as necessary to sustain U.S. dominance in global AI capability. The private sector has acted with more alacrity but in a less coordinated fashion.

In terms of levels of analysis, the difficulty in translating national plans into action at lower levels, sits within the second level of debate, highlighting systemic characteristics relating to how government funding flows and where responsibility lies. The next paragraph shows how private sector organisations have shown greater agility.

Over the past decade, the US private sector, including non-state universities, has committed resources to expansion of the AI sector (including university-based and internal R&D, infrastructure, and workforce expansion) on a scale unmatched by any other country. Stanford's 2025 *AI Index* estimates that US private AI investment reached about US\$109.1 billion in 2024, nearly twelve times China's \$9.3 billion and twenty-four times the UK's \$4.5 billion, with much of this spending directed to 'enablement, talent, and upskilling' in addition to infrastructure (Stanford 2025, 4). In the following year, the US extended its lead, with "nearly \$285.9 billion total invested, 23.1 times greater than the amount invested in the next highest country, China (\$12.4 billion), and 48.5 times the amount invested in the United Kingdom (\$5.9 billion)" (Stanford 2026, 182).

Individual philanthropists and institutions have made similarly outsized investments. Dating back to 2018, Stephen Schwarzman's US\$350 million gift to MIT, part of a broader US\$1 billion commitment, enabled the creation of the MIT Schwarzman College of Computing. Its initial concept was to set up a new faculty of AI, not to research the subject in the abstract, but to research how AI could enable other fields of academic research, its aim was to 'bring the power of computing and AI to all fields of study' (Mervis 2018, Schaffhauser 2018). The plan was to double MIT's computing faculty by roughly 50 positions, making it one of the most imaginative and structurally transformative AI-education investments anywhere in the world. Individual philanthropy is a much more common characteristic of the US system than in the UK or Australia, having an impact on the funding of educational institutions and finance of innovation.

In parallel, major US tech firms have pledged more than US\$2 billion specifically for AI education, including Google's US\$1 billion programme to provide AI training and career certificates to US college students (Inside Higher Ed 2025), and OpenAI's funding of a National Academy for AI Instruction to train around 400,000 K-12 teachers (AFT 2025).

Some of the largest firms have launched internal AI-related upskilling programs on a scale measured in hundreds of millions or even billions of dollars (Dawson 2020, Westover 2025). Amazon's "Upskilling 2025" initiative, announced in 2019, committed US\$700 million to train 100,000 US employees (roughly one-third of its US workforce) into higher-skilled, often AI-adjacent roles via internal programs like Machine Learning University and Technical Academy (Dawson 2020). AT&T's "Future Ready" programme similarly invested about US\$1 billion over several years to provide its workforce with new technical skills, including AI and data science, through partnerships with Coursera, Udacity and leading US universities. More recently, financial-sector firms such as Citigroup have introduced mandatory AI prompt-engineering and AI-literacy training for 175,000 employees across 80 locations, and comparable enterprise-wide AI-training efforts are reported at JPMorgan Chase and other major banks (Westover 2025). Surveys of leading companies show that a growing number of them now run dedicated AI-learning programmes for all employees (such as KPMG's "GenAI 101" and "Trusted AI" courses) rather than confining AI skills to technical teams (Kitterman 2025). The upskilling interest in the private companies is not matched by an effort to define a role for academic institutions but is usually handled using internal corporate resources. This could lead to industry or even vendor specific expertise that is not useful in growing a national workforce.

By 2026, several major universities and large firms were offering free online courses in the foundations of AI. For example, Harvard was offering a seven week course the CS50AI "Introduction to Artificial Intelligence with Python" (Harvard n.d.). The project-based course covers the "theory behind graph search algorithms, classification, optimisation, reinforcement learning, and other topics in artificial intelligence and machine learning as they incorporate them into their own Python programs". The aim is to offer experience in libraries for machine learning and knowledge of AI sufficient to "design intelligent systems of their own". The only prerequisite is experience in Python programming, and nationalist exclusions may not extend to students from countries like China, Iran and Sudan

At the same time, in spite of these initiatives, aggregate data suggest that most workers remain under-trained in AI. A 2026 enterprise survey synthesised by Go1 reports that only about 35 per cent of employees have received any formal AI training, even though 94 per cent of CEOs say AI skills development is a strategic priority (Go1 2026). The same analysis estimates that the global AI skills gap costs businesses roughly USD 5.5 trillion in lost productivity, while firms that do invest in structured AI training see an average return of US\$3.70 per dollar spent, with trained employees being 2.7 times more proficient in AI use than self-taught colleagues. Workforce-readiness surveys in the US echo this picture, with

one 2025 study finding that 79 per cent of workers feel unprepared to use AI at work, suggesting that even in a country with high overall private AI investment, sustained and broad-based internal training still lags behind demand (Bright Horizons 2025). These findings indicate that large US firms are beginning to scale AI upskilling aggressively, but that such efforts currently reach only a fraction of the workforce. Moreover, we have analysis of the contribution such programmes make, their intensity or their level of education.

The 2026 Stanford index report concluded that “demand for AI skills is rising across sectors but the workforce impact is showing signs of falling disproportionately on the youngest workers in AI-exposed occupations” (Stanford 2026, 171).

The dynamics in the survey data show above sits with the third debate between enterprise and employee in our level of analysis. It highlights barriers to employee training within enterprises which may speak to a wide variety of factors such funding, capacity in the company, capacity in educational providers and speed of change. Another worrying indicator on the impact on early stage careers is noted.

Taken alone, these developments do not demonstrate AI cyber readiness. Their relevance is indirect but important: they expand the institutional and financial base from which cyber-specific AI capability, education, and tooling may be built.

Moving away from AI in general to the cyber security impacts, US public discourse paints the analysis as very much a work in progress that did not gain much momentum until 2025. The scene from earlier years is instructive. A governmental workforce strategy in 2023 merely flagged AI as of interest (White House 2023) with only two instances of the abbreviation AI. A survey-based report by ISC<sup>2</sup> found that most practitioners (88 per cent) expected AI to change and redefine many cyber security roles, removing people from some high-speed and repetitive tasks (ISC<sup>2</sup> 2024a, 3). Many anticipated redeployment of staff toward more complex analysis and oversight of AI-driven tooling (p.11). The majority (56 per cent) believed that AI would make some part of their job obsolete. The report emphasises that AI will not eliminate the need for human cyber professionals but will shift skill requirements toward higher-order judgement, model tuning and cross-domain collaboration. The report noted that “as the technology is still in its infancy, education is paramount” (p. 11). The survey was executed in 2023 based on 1123 respondents.

In 2024, ISC<sup>2</sup> dedicated that year’s annual report on the cyber workforce, to likely changes under the impact of AI (ISC<sup>2</sup> 2024b: 4). However it concluded that while firms have ambitious plans for AI, they “are not immediately overhauling their practices to adopt AI”. This is based on their assessment that the “biggest return on investment [in AI cyber] will occur in two or more years”. The report further observed that “cannot yet predict what activities, if any, AI will replace” and “hiring managers aren’t rushing to hire more specialised workers”, focusing instead on “nontechnical skills like problem-solving that will be transferable through the increased use of AI” (p. 6).

It is also worth pointing out that the adoption of AI and associated skills is not the same as adopting a widescale radical change in business models and processes. There is little so far that adds to our understanding of Scenario 3, with coverage over the period 2021-2025 being focused on Scenarios 1 and at most hybrid skills in Scenario 2. However, it must be remembered that this is also a period during which the commodification of generative AI has had a huge impact on both individuals and business users. This is an indicator of the acceleration of the speed of change as picked up in the next paragraph.

Even so, the pace of adoption of AI was creating challenges for cyber security professionals. Almost half of cyber security teams had already incorporated Gen AI into their toolsets to “bridge skills gaps, improve threat detection and provide vast benefits to cybersecurity”. In comparison, a higher share of non-cyber work teams had incorporated Gen AI into other departments, “causing more work for cyber professionals” and stimulating data privacy and security concerns” due to AI among the cyber workforce (p.7).

Activity in the enterprise system is causing more work for cyber staff – a good example of where system dynamics are driven by, in this instance a, new technology which in turn drives the behaviour of individuals (the third debate).

The 2025 ISC 2 workforce study represents a landmark overview. It found that most practitioners see AI as a career booster: 73 per cent believe AI will create more specialised cyber skills, 72 per cent see a need for more strategic mindsets, and about two-thirds expect broader skillsets and more communication-heavy roles (ISC<sup>2</sup> 2025: 25-6). (The poll surveyed 16,029 cyber security practitioners and decision-makers from across North America, Latin America, the Asia-Pacific region and Europe, the Middle East and Africa (p.3). Since 34 per cent of respondents were from the US (p. 47) this allows a reasonably sized sample of respondents but there is no ways of cross-referencing the national status or location to professional roles or qualifications.

A short policy-oriented assessment from a 2025 report from the Business Executives for National Security (BENS), addresses what it calls “The Cybersecurity Workforce Gap: Confronting National Security Risks in the AI Era” (BENS 2025). It concludes that the US defensive cyber capabilities will be unable to keep pace with evolving information warfare without a much deeper bench of cyber professionals who are AI-proficient. It cites a US cyber-workforce deficit of about 522,000 roles, with “particularly acute shortages” in “AI-enabled cybersecurity” and other highly technical areas, at exactly the time when adversaries are accelerating AI-based capabilities. The report argues that “many cyber defence functions that once relied on human intervention must now be fully automated, further shifting the demand toward highly technical, AI-proficient expertise,” and calls for AI-aware workforce strategies including early STEM engagement, public-private training partnerships and accelerated clearance processes.

Beyond strategy documents and studies, some national-scale programmes explicitly combine AI and cyber workforce development. At the University of New Haven, the NSA/NCAE-C Immersive Cybersecurity Workforce Development Program (ICWDP), recruiting cohorts through 2025–2026, to prepare individuals for AI, cybersecurity, and cyber threat analyst jobs” (University of New Haven n.d.). At the University of West Florida, a National Cybersecurity Workforce Development Program funded by DoD/NSA, highlights AI, Python and threat intelligence as core components (CyberSkills2Work 2025). These show a shift toward AI-enabled cyber operations skills.

### *Role changes at the coalface in the US*

This section gives some insights into changes in job specifications and corresponding adjustments in statement of required skills and qualifications in the US. This is only possible at a bare-bones or general level due to data limitations and the hundreds of different roles in AI-enabled cyber operations relating to security (defence, offence, deterrence and mitigation). There is a similar coalface sub-section in the treatment of the UK and Australia.

Since 2024, job descriptions for cyber security roles in the United States have changed in response to the growing use of AI by emphasizing AI literacy, human oversight of

automated systems, and a broader mix of technical and governance capabilities (ISC<sup>2</sup> 2025; Jepma 2025). Rather than treating AI as a niche or optional specialty, employers increasingly appear to frame it as a routine part of cyber security practice, especially in threat detection, response automation, and risk management (Goh 2025). This shift has altered not only the skills listed in role descriptions, but also the way work itself is defined across operational, analytical and strategic security functions (ISC<sup>2</sup> 2025). On the other hand, one survey reported a “concerning trend of cybersecurity teams being excluded from the development, onboarding and implementation of AI solutions” in 2024 (Goh 2025).

The US Government (notably NSF and DoW/NSA) has recognized the dual relationship between AI and cybersecurity (cybersecurity of AI and AI use in cybersecurity) by funding the development of a new set of curriculum content called Stoneman that was developed and is currently tested in universities across the US.

This paragraph sits with the third level of debate between enterprise/ bureaucracy and the individual, as it relates to specific job specifications. The case can be made for this approaching Scenario 2 in terms of hybrid skills. The comment regarding the exclusion of cyber security specialists from onboarding of AI, outside of this particular context, could be for a variety of reasons such as:

- an indicator that hybrid roles are shared with others and that whose job it is, is not a settled matter. Indeed, AI developers may not see cyber security people as having an assurance role at this or any stage
- An indicator that cyber security roles are not yet the natural home for assuring technologies developed in adjacent areas such as data science and engineering.

One of the clearest changes has been the movement of AI literacy into mainstream cyber security skills requirements. Industry evidence from 2025 shows that AI-related capability is now widely seen as essential for digital trust and cyber professionals, with 72 per cent of respondents in ISACA’s AI Pulse Poll stating that AI skills are very or extremely important in their field, and 89 per cent saying they will need AI training within two years to retain or advance in their roles (ISACA 2025). The 2026 ISACA poll found some modest increase in these percentages (ISACA 2026). US cyber job descriptions are increasingly rewarding applicants who can work confidently with AI-enabled platforms and workflows (Jepma 2025). The headline assessment of the 2026 ISACA poll was that “AI adoption is accelerating faster than AI readiness”.

A second major shift has been in the balance between “manual” and supervisory work. AI is reshaping entry-level cyber security jobs by reducing the share of repetitive tasks that previously formed the basis of junior security work, including first-level monitoring and basic analysis (Ross 2025). As these functions become more automated, job descriptions increasingly stress the need to interpret AI-generated alerts, validate outputs, recognise limitations in automated recommendations, and escalate complex incidents using human judgment rather than simply processing large volumes of low-level data (Ross 2025; Lee 2025). In practical terms, this means that junior roles are being redefined away from purely routine detection work and toward quality assurance, investigation and human oversight of AI-assisted systems (Ross 2025).

A third development is the appearance of new and more specialised role categories associated with securing AI itself. Analysis of vacancies published in 2025 and 2026 identify emerging job titles such as AI Security Analyst, Machine Learning Engineer for Security, AI Governance and Ethics Officer, and Synthetic Threat Analyst (Lee 2025). These roles typically require familiarity with machine learning concepts, data pipelines, adversarial attack methods, governance controls, and compliance issues associated with enterprise AI deployment (Lee 2025). More broadly, the ISC<sup>2</sup> Cybersecurity Workforce Study indicates

that practitioners expect AI to create more specialised roles and broader skill requirements rather than simply eliminate jobs (ISC<sup>2</sup> 2025).

Overall, since 2024, US cyber security job descriptions have evolved to reflect a profession in which AI is not yet replacing cyber workers outright but is increasing demand for professionals who can combine cyber security expertise with AI fluency, interpretive judgment, and governance awareness (ISC2 2025; da Gama and Perucica 2025).

In US cyber roles, references to AI sub-fields are emerging but uneven. Workforce and career analyses show employers increasingly asking for “machine learning” and “AI/ML security fundamentals” in security engineer and AI security specialist roles, and sometimes explicitly mentioning adversarial machine learning or AI model security. Respondents in the 2025 ISC<sup>2</sup> study identify five priority AI/ML competencies for cyber professionals: using AI in threat detection and response (42 per cent), applying AI in threat modelling and risk assessment (39 per cent), defending AI models from attack (35 per cent), securing AI integrations in cloud and edge environments (31 per cent), and developing or implementing AI governance and policy frameworks (30 per cent). Each of these maps onto particular AI sub-fields: the first two to supervised/unsupervised ML and anomaly detection; the third to adversarial ML and model-security techniques; the fourth to applied ML and systems-engineering skills in distributed environments; and the fifth to cross-cutting governance of generative and other high-impact models.

Other anecdotal assessments may be useful:

- A 2026 workforce report on cyber leaders concludes AI is shifting leadership from technical execution to oversight and accountability; leaders report heightened expectations for cross-department collaboration, communication with executives, and governance of AI-driven security (Business Wire 2026)
- AI “solves lower-level problems” but does not replace staff; organisations must invest in upskilling existing teams, because human understanding of context and configuration remains indispensable (Short 2025).
- AI is raising the bar for cyber jobs: entry-level, repetitive roles are being compressed, while higher expectations are placed on newcomers to understand AI tooling, focus on “real” in-demand skills, and build evidence of experience.
- AI is reconfiguring, not shrinking, the workforce – expanding strategic, communicative and governance-heavy leadership roles, and demanding deeper multi-domain skillsets from practitioners.

## Workforce reform for AI cyber in the UK

The United Kingdom stands out for its potential to explicitly measure AI adoption and AI-related skills within its cyber security workforce though its data on AI skills is not especially granular before 2025. The UK Department for Science, Innovation and Technology’s (DSIT) has undertaken an annual analysis of cyber security skills in the UK labour market since 2018 (UK DSIT 2025a). For most of that time, the main study (a Findings Report) has been accompanied by a Technical Findings report (UK DSIT 2025b). The 2024 Findings Report saw AI skills as largely a future question: “the need for skills to understand and act upon AI tools, roles becoming ‘AI cyber’ rather than just ‘cyber’ and the emergence of deeper specialisations such as ‘cyber security machine learning’”. Almost all mentions of AI in were in a chapter on future workforce needs (UK DSIT 2024a).

According to DSIT’s 2025 findings, 53 percent of UK cyber security businesses report that their staff use AI tools in day-to-day work (DSIT 2025a: 4). At the same time, 65 percent of these businesses expected a need for AI-related skills to increase over the subsequent 12 months. Despite this, only 42 percent have provided any AI training to their staff. This

combination of high and growing use of AI tools paired with relatively low levels of formal AI training suggests a significant AI skills gap within the UK cyber workforce. In 2025, “1,335 out of the 32,370 job postings [for core cyber jobs] (4 per cent) explicitly requested AI skills” (p. 29). A section of the 80-page annual report that was dedicated specifically to coverage of AI skills for cyber security was only three pages in length.

The DSIT report also provides qualitative insights into how employers perceived AI would impact on cyber roles. Many firms report that AI increases demand for higher-order analytical capabilities, including the ability to interpret AI-generated threat intelligence, understand and manage AI-driven detection systems, and assess AI-related risks (UK DSIT 2025a: 51). Employers express concern that shortages in these AI-related skills could limit their ability to leverage AI for defence and to manage AI-enabled threats. This aligns with broader UK analyses suggesting a shift in demand from purely technical or operational tasks towards hybrid roles that combine technical grounding with strategic, governance and risk-management competencies.

The UK situates AI-for-cyber workforce issues within a wider AI skills policy framework. The “AI Skills for Life and Work” summary report, for instance, emphasises the need to build AI literacy across the general workforce, while also supporting more advanced AI skills in key sectors, including cyber security (UK Department for Education & DSIT, 2026). It highlights that employers often lack confidence in their ability to identify and develop AI-related competencies, and calls for targeted interventions in education, training and professional development to close emerging gaps. In this context, cyber security is framed as one of several domains where AI literacy and specialised AI capabilities must be developed in tandem.

Industry and sectoral analyses reinforce DSIT’s findings. Commentary from cyber industry bodies notes rapid growth in the UK cyber security workforce but points out that organisations are struggling to keep pace with evolving skill requirements, particularly around AI-enabled detection, automation and response (Cyber Exchange UK 2025; FinTechWales 2026). Some reports underscore that while AI tools can help alleviate pressure on over-stretched cyber teams, they also require investment in new skills – such as configuring, monitoring and auditing AI systems – that are not yet widely available. This mirrors DSIT’s observation that AI adoption in cyber businesses often outpaces formal training, potentially creating operational and governance risks.

The UK exhibits an explicit data-rich approach to understanding how AI is reshaping its cyber workforce. National-level surveys quantify AI tool usage and training within cyber businesses, and policy documents explicitly recognise AI-related cyber skills as a distinct area of concern (Department for Science, Innovation & Technology, 2025; UK Department for Education & DSIT, 2026). However, similar challenges remain: employers still report shortages of AI-related competencies, and there is an emerging need to translate high-level strategies for AI skills into concrete curricula, qualifications and career pathways for cyber professionals.

UK labour-market statistics speak about “AI tools” in aggregate, but qualitative findings and industry reports reveal how particular sub-fields are shaping cyber work. DSIT’s annual cyber security skills report for 2025 does not break down AI usage by sub-field, yet employers consistently highlight AI-enabled detection, automation and response as key drivers of skill demand (DSIT 2025a). This implies widespread deployment of supervised and unsupervised machine learning, including anomaly detection and classification models, into SOC environments, threat-hunting and vulnerability-management processes.

At the same time, UK commentary on AI governance and skills, such as the Skills for Life and Work report, emphasises the need for competencies in understanding, interpreting and overseeing AI systems, including risk assessment and transparent use of LLM-based tools (UK Department for Education & DSIT 2026). Up to 2025, while sub-fields such as NLP and LLMs are not explicitly named in the DSIT cyber workforce surveys, industry observers note their growing use in phishing detection, log and alert triage, and threat-intelligence summarisation. The rise of AI governance and compliance expectations also creates latent demand for roles focused on model-risk management, adversarial robustness and oversight of generative-AI use, even if these are not yet formally distinguished in national role taxonomies (Cyber Exchange UK 2025; FinTechWales 2026).

A distinct data series provides more granular analysis. DSIT (2025c) published an analysis of the market for software and AI cyber security services. It found 66 firms in the UK providing cyber security for AI systems, of which 14 focused exclusively on AI cyber security and 52 wider cyber security firms providing AI security capabilities. DSIT (2026) updates those figures. It assessed 111 UK-registered firms offering cyber security for AI systems either a product or service (DSIT 2026). It noted that this represented an “increase of 45 firms (+68 per cent) since the previous baseline”. Of these, 32 were “specialist providers focused primarily or exclusively on cyber security for AI.”

The 2026 report on software and AI cyber offered a breakdown by AI sub-field or specialisation: AI/ML model security (57 per cent), AI security advisory and consulting (43 per cent), and AI runtime and infrastructure security (41 per cent) are the most commonly cited offerings (DSIT 2026). AI red teaming and penetration testing has emerged as a distinct service category (21 per cent), and nascent areas such as agentic AI security (5 per cent) and AI browser/endpoint security (5 per cent) are responding to the increased rollout of AI agents in enterprise environments.

In short, the UK has the most detailed national data on the extent of AI use in cyber businesses. Differentiation by sub-field is more visible at the level of industry tools and emerging job descriptions than in government workforce measurement. The challenge for UK workforce planners will be to move from AI usage in cyber as a single metric to more granular indicators that capture how machine learning, LLMs, generative AI and other sub-fields map onto distinct roles, skills and training needs.

### *Role changes at the coalface in the UK*

Since 2024, job descriptions for cyber security roles in the United Kingdom have evolved under the combined influence of rapid AI adoption, a tightening but still growing labour market, and policy emphasis on advanced digital skills (DSIT 2025a; techUK 2024). Government monitoring of the skills landscape shows that while the UK cyber workforce expanded to around 143,000 by the end of 2024, employers increasingly expect candidates to possess higher-level capabilities, including the ability to work with AI-enabled tools and data-driven security processes (DSIT 2025a). This has occurred against a backdrop of falling advertised vacancies and fewer explicitly “entry-level” opportunities, suggesting that job descriptions are skewing towards mid-career roles with broader and more sophisticated skills profiles (DSIT 2025a).

A central feature of this shift has been the move from generic “cyber” skills towards hybrid profiles where AI literacy and data competencies are more explicit. The 2024 and 2025 annual Cyber security skills reports note that the growing deployment of AI in cyber operations is expected to drive four major changes: increased automation of cyber tasks, a need for skills to understand and act on AI tools, an evolution of roles from “cyber” to “AI cyber”, and the emergence of specialisations such as “cyber security machine learning”

(DSIT 2024a, 2025a). Accordingly, job analysis within these reports finds strong demand for skills in governance, risk management, secure architecture, data protection and cyber threat intelligence, but with an increasing overlay of analytical and AI-related competencies, particularly in larger and more mature organisations (DSIT 2025a).

From a labour-market perspective, job postings data also suggest a qualitative shift in role definitions. Between 2022 and 2024, the share of UK postings seeking candidates with less than one year of experience fell from 25 per cent to 17 per cent, while almost two-thirds of core cyber job ads required mid-level experience (DSIT 2025a). This pattern is consistent with recruiters' observations of a more specialized job market, in which "bread and butter" roles in areas such as general governance, risk and compliance have declined and been partially replaced by more niche posts aligned with operational resilience, regulation and technology-specific expertise (Barclay Simpson 2025).

As AI tools become embedded in monitoring, incident response and resilience work, advertisements for these mid-level roles increasingly expect practitioners to operate and supervise AI-enabled systems rather than perform all monitoring and analysis manually (techUK 2024; Scroxtion 2026).

At the strategic level, national policy has reinforced this trend by framing cyber security capability as inseparable from advanced digital and AI skills. The UK's skills strategy and related cyber initiatives emphasise the need for a "sustainable supply of home-grown cyber skilled professionals" able to adapt to an AI-driven threat environment, including through education and reskilling programmes that integrate AI, data and cyber content (UK Cyber Security Council 2025). Recent commentary highlights that by 2030 AI is expected to drive "immense change" in the UK cyber profession, with employers urged to invest now in training staff to work effectively with AI tools rather than merely adding ad hoc automation requirements to job descriptions (Scroxtion 2026).

Overall, since 2024, UK cyber security job descriptions have begun to shift away from generic security profiles towards roles that assume familiarity with AI-enabled tools, prioritise mid-level experience, and increasingly blend cyber security expertise with data-analytic and AI-related competencies (DSIT 2025; techUK 2024). At the same time, according to advertisements on UK jobsite Indeed, detailed AI sub-fields are rarely spelled out in cyber security postings outside highly specialised roles, the main exceptions being the banking industry or research organisations.

## Workforce reform for AI cyber in Australia

In Australia, policy and labour-market analysis increasingly recognises that AI will reshape both cyber threats and cyber security work, but the intersection of AI and cyber security is still treated mainly as part of a broader digital and AI skills agenda rather than as a distinct workforce stream. Recent national-level documents emphasise overlapping data, digital and cyber capabilities as key pillars of future workforce development, with AI positioned as a general-purpose technology that cuts across these domains rather than as a discrete cyber-specialisation (Jobs and Skills Australia, 2025). The report does not mention "cyber" at all and only mentions security in a generalised fashion. For example, its only mention of the cyber security scene, is this: "When AI tools are used without employer oversight, responsibilities related to data security, ethical use and compliance may shift onto individual employees, who may not be equipped to navigate these risks" (p. 82). The National AI Plan has no consequential or detailed mentions of cyber security except for motherhood statements about existing commitments with no elaboration of the connection with AI.

More explicit links between AI and cyber workforce development appear in public-sector planning. The Australian Public Service Commission's *Data, Digital and Cyber Workforce Plan 2025–30* outlines a strategy to build and retain a workforce capable of using data effectively, delivering digital services and managing emerging technologies (including AI) across government (Australian Public Service Commission 2025). The plan notes that the adoption of AI and related technologies will increase demand for skills in secure digital service delivery, risk management and resilience, and that cyber professionals will need to understand AI-driven systems as part of their remit. However, AI-specific cyber roles are not yet codified as distinct occupational categories. AI is framed as an enabling technology that existing data, digital and cyber roles must learn to use and govern.

Complementary work by the government on AI skills reinforces this broad framing. The forthcoming report on *AI, Digital and Workforce Futures* is tasked with examining how AI is being used across the Australian economy and what capabilities workers require to use it safely and productively (Skills Insight, 2026). Cyber security is treated as a cross-cutting safety and resilience concern within this analysis, rather than as a stand-alone AI-for-cyber track. Sectoral analyses, such as studies of generative AI's impact on workplace skills and reports on Australians' use of AI at work, suggest that higher-skill occupations – including security roles – will see significant task change and increased emphasis on interpreting AI-generated outputs, but again stop short of defining a dedicated AI cyber workforce architecture (Tech Council of Australia, 2025).

From a security-operations perspective, the Australian Signals Directorate's annual cyber threat report for 2025 highlights the growing use of AI by adversaries and in defensive tooling, noting that AI-enabled phishing, social engineering and automated vulnerability discovery are becoming more prevalent (Australian Signals Directorate 2025). The report implies a need for defenders who understand both how AI can be weaponised and how it can support detection and response, but it concentrates on threat landscape and operational case studies rather than detailing workforce planning or skill taxonomies.

Public documentation offers limited granularity on how many cyber roles now involve AI-based tools, what proportion of cyber staff receive AI-specific training, or how rapidly AI-centric tasks (such as securing AI models or governing AI use) are diffusing through the cyber workforce.

Overall, Australia can be characterised as strong on high-level AI and digital workforce framing but relatively under-developed in explicitly articulating AI cyber workforce development. National reports emphasise the importance of cyber security and AI separately. As of 2025–26, there is limited publicly available detail on AI-specific cyber roles, training coverage, and progression pathways, suggesting an opportunity for more systematic workforce analysis and program design.

In summary, Australian policy documents rarely distinguish AI sub-fields explicitly in workforce terms, but their language and examples imply particular emphases. They acknowledge that AI will change cyber work and highlight generative AI and automated detection as important trends, but do not yet codify distinct roles or training pathways aligned with specific AI sub-fields, such as securing machine-learning models in production, governing organisational use of LLMs or managing computer-vision systems in industrial and critical-infrastructure environments.

### *Role changes at the coalface in Australia*

Job descriptions have shifted in response to strong and sustained demand, regulatory tightening and the rapid integration of automation and AI into security operations (Jobs

and Skills Australia 2025; e2 Cyber 2025). Specialist recruiters report that the “biggest change in the market is not just volume, but intent,” as organisations move from reactive threat response to proactive investment in cyber resilience and strategy (e2 Cyber 2025). This has driven job descriptions away from narrow operational remits and towards roles that explicitly combine technical skills, governance and strategic advisory capabilities, often in AI-enabled environments (e2 Cyber 2025; Burke 2025).

One major development has been the growing prominence of governance, risk and compliance (GRC) and identity-focused roles. Analysis of Australian vacancy data for 2024–25 shows that GRC roles re-emerged as the single largest category of open cyber security positions, accounting for roughly 26.2 per cent of all roles by late 2025 and overtaking security engineering and security operations for the first time since 2022 (Burke 2025). This reflects what some commentators describe as a shift from “growth at all costs” to “control at all costs,” as organisations respond to heightened regulatory expectations, major breach experiences and new compliance obligations (Burke 2025; e2 Cyber 2025). In job descriptions, this is visible in the increasing weight placed on skills in risk assessment, audit readiness, identity and access management, and regulatory interpretation, often alongside technical familiarity with automation and analytics tools (e2 Cyber 2025).

AI and automation are also reshaping how technical and architectural roles are defined. Market analysis for 2025 emphasises a “strong push towards automation and predictive analytics,” with cyber professionals now expected not only to protect systems but to “build intelligence into the way those systems behave” (e2 Cyber 2025). Employers therefore increasingly seek Australian candidates who can operate between tools, technology and strategy, with particular demand for skills in cloud-native security, Zero Trust architecture, threat intelligence and AI-enabled monitoring (e2 Cyber 2025; Decipher Bureau 2025). The emergence of new statistical records employment codes such as “Cyber Security Engineer” and growing investment in operational technology security, secure coding and AI ethics micro-credentials further illustrate how job descriptions now reflect more specialised and AI-relevant competencies than in the early 2020s (ACS 2024; e2 Cyber 2025).

Public-sector workforce planning and regulatory developments reinforce this trajectory. The APS Data, Digital and Cyber Workforce Plan 2025–30 highlights enterprise architects, cyber security analysts and IT/data architects among the top ten in-demand roles and calls out the need for stronger data and digital skills across the Commonwealth workforce (Australian Government 2025). Parallel regulatory changes – including privacy reforms and the continued enforcement of legislation on the security of critical infrastructure – have been reflected in job descriptions that stress strategic risk management, privacy-security integration and uplift of cyber maturity rather than narrow technical task lists (e2 Cyber 2025; Australian Signals Directorate 2025). Overall, between 2024 and 2026, Australian cyber security job descriptions have evolved towards hybrid profiles that combine strong technical capability, governance and compliance expertise, and the ability to design, operate and explain increasingly automated and AI-supported security environments (Jobs and Skills Australia 2025; e2 Cyber 2025).

While the trends are clear, the numbers are very low. Since 2022, Australian government job advertisements that mention AI-related work (including cyber security) have reached a plateau, at 200 or fewer per year (Awarded Contracts, 2026). In the years since 2020 inclusive, the federal government hired 880 people for AI/ML related roles. Around 38 per cent of those jobs were in national security related agencies (such as Defence, ASD, Home Affairs, ASIO and eSafety). As one illustration of the low number of jobs available, on 7 May 2026, the national jobs website, Seek, was advertising only eight jobs linking “cyber security” and “machine learning”, of which two were for academics, two for government and three for the private sector. The age of the postings was between 5 and 29 days. By

contrast. Those listing “machine learning” on the same day without a mention of security numbered 283.

Australian evidence shows that cyber-specific job descriptions usually reference AI as part of broader automation and analytics capability rather than by sub-field, although the national skills datasets do track fine-grained AI skills in the wider labour market. Jobs and Skills Australia’s emerging-roles analysis identifies an AI skill cluster that includes image and voice recognition, intelligent control, AI operations and related techniques, but notes that these skills are more prominent in technical AI and data occupations than in general roles, indicating a slower uptake of highly specific AI skills in typical job ads.

## Trilateral comparisons

The trilateral comparison is not a ranking exercise. It is an assessment of how differently placed national systems are to observe, interpret, and respond to AI-driven change in cyber security work. Scholarly and professional sources together suggest a clear differentiation between the three countries along two dimensions: (1) the explicitness of AI cyber workforce planning and measurement, and (2) the degree to which AI sub-fields are recognised in competencies and roles.

On the first dimension, the UK leads in systematic measurement, providing national statistics on AI use and training in cyber businesses, albeit with AI treated as a single category. The US leads in competency-level profiling of AI-related cyber skills, particularly around threat-detection ML, adversarial ML and AI governance, via professional surveys. Australia, by contrast, embeds AI cyber themes in broader digital and AI workforce strategies and relies more on general labour-market reports and sectoral analyses than on dedicated AI cyber surveys.

On the second dimension, the US exhibits the most explicit alignment between sub-fields and competencies, with skills categories that clearly map onto ML-based detection, model defence and governance. The UK shows implicit sub-field differentiation in practice – ML-based detection and emerging use of LLMs – but still aggregates AI cyber roles with little sub-field differentiation. Australia acknowledges ML-based detection and generative AI in threat reports and skills studies but has yet to reflect these distinctions in workforce taxonomies.

Across all three countries, scholarly literature on AI-for-cyber underlines that these sub-field distinctions matter. Reviews of AI and ML in cyber security emphasise anomaly-detection models, NLP systems and generative models. Each entails different vulnerabilities and operational challenges, requiring distinct skill sets in model development, evaluation and governance.

The comparative evidence indicates that advanced economies are still at an early stage in aligning their cyber security workforces with the demands of AI sub-fields. The US has made the greatest progress in articulating competency clusters that correspond to distinct AI applications in cyber security, while the UK has set fairly broad benchmarks for measuring AI usage and training levels in the cyber labour market. Australia has begun to recognise the effects of generative AI and AI-driven detection on security tasks, even if workforce frameworks remain largely agnostic about sub-field specialisations.

The key implication is that future policy and research should move beyond generic references to “AI skills” and engage directly with AI sub-fields when designing curricula, qualifications and workforce strategies. Doing so would support more realistic planning for roles such as anomaly-detection engineers, adversarial-ML specialists, AI-governance leads

and AI security engineers. Without this nuance, there is a risk that national strategies will under-specify the capabilities needed to manage an AI-saturated threat environment, despite recognising AI's importance in general terms.

## Conclusion

This paper points to the value of a matrix approach in considering levels of analysis rather than a single-level approach. Most strikingly, the individual level and the international system level are interacting directly in all three countries, bypassing both state and sub-state levels. The decisions of individual AI developers at US-headquartered firms (Microsoft, Google, Anthropic, OpenAI) are reshaping both the threat landscape and the defensive toolset available to cyber professionals in the UK and Australia faster than any national workforce strategy can respond. This is precisely the kind of non-adjacent interaction that the paper's matrix approach identifies as theoretically significant, and it has direct practical implications: national workforce planning frameworks that operate only at the national level will systematically underspecify the skill requirements generated by technology adoption decisions made at the individual and enterprise level in another jurisdiction.

A second non-adjacent interaction runs between the sub-state level (enterprises and universities) and the international system. The rapid growth of UK-based AI cyber firms from 66 to 111 between 2025 and 2026 (DSIT 2025c; DSIT 2026) reflects enterprise-level commercial decisions responding to international market signals, not national workforce strategy. Similarly, the decisions of US private universities and philanthropists (the MIT Schwarzman College of Computing, Google's US\$1 billion AI training programme) are shaping the international supply of AI-capable cyber talent in ways that Australian and UK national-level planning did not anticipate and cannot easily replicate. The Hollis and Smith framework, used tiered debates sequentially, would locate these dynamics either in the national-bureaucracy debate or in the bureaucracy-individual debate; the matrix approach reveals that they are simultaneously operating across all four levels.

The comparison also reveals important differences in the dominant level at which reform is occurring in each country. In the US, the primary drivers of AI cyber workforce development are at the sub-national and individual levels (private investment, corporate upskilling, philanthropic endowment) with the national government playing a supporting and partially compensatory role. In the UK, the state level is the primary site of measurement and strategic framing, with sub-national actors adapting relatively responsively to that framework. In Australia, by contrast, the dominant dynamic is at the international system level (exposure to the same global AI capability curve as the other two countries) without the sub-national investment density of the US or the measurement infrastructure of the UK. This produces the "strong on framing, thin on implementation" pattern that the Australian section of this paper documents.

## References

- ACSC (Australian Cyber Security Centre) (2024) Engaging with artificial intelligence, Canberra: Australian Government, <https://www.cyber.gov.au/business-government/secure-design/artificial-intelligence/engaging-with-artificial-intelligence>
- AFT (2025) AFT to Launch National Academy for AI Instruction with Microsoft, OpenAI, Anthropic and United Federation of Teachers (6 July 2025), <https://www.aft.org/press-release/aft-launch-national-academy-ai-instruction-microsoft-openai-anthropic-and-united>
- AI Exposure Institute (2026) The government's AI workforce response: Too little, too late? <https://www.aiexposure.org/analysis/government-response-ai>
- Awarded Tenders (2026) The Government AI Workforce: Six Years of Hiring Data Reveal Two Parallel Professions, <https://awardedtenders.au/articles/awardedtendersau/market-insights/ai-workforce-federal-government-2020-2026/>
- Ashfin U (2024) 'Artificial intelligence for cybersecurity: literature review and future directions', *Frontiers in Computer Science and Artificial Intelligence*, 3(1), pp. 15–25, <https://al-kindipublisher.com/index.php/fcsai/article/view/11441>
- Austin G. (2020) Twelve Dilemmas of Reform in Cyber Security Education, in Greg Austin (ed), *Cyber Security Education: Principles and Policies*, Routledge, 2020, pp. 208-221
- Australian Public Service Commission (2025) Data, Digital and Cyber Workforce Plan 2025–30, [https://www.dataanddigital.gov.au/sites/default/files/documents/2025-10/APS%20Data%2C%20Digital%20and%20Cyber%20Workforce%20Plan%202025-30\\_v1.1.pdf](https://www.dataanddigital.gov.au/sites/default/files/documents/2025-10/APS%20Data%2C%20Digital%20and%20Cyber%20Workforce%20Plan%202025-30_v1.1.pdf)
- Australian Signals Directorate (2025) Annual Cyber Threat Report 2024–2025, <https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025>
- Bain & Company (2025) AI: The ambitions are bold, but the talent is scarce, 23 February 23, <https://www.bain.com/insights/ai-the-ambitions-are-bold-but-the-talent-is-scarce-snap-chart/>
- BENS (Business Executives for National Security (2025) The cybersecurity workforce gap: Confronting national security risks in the AI era, <https://bens.org/the-cybersecurity-workforce-gap-confronting-national-security-risks-in-the-ai-era/>
- Bright Horizons (2025) AI workforce readiness crisis: 79 per cent of workers say they're not ready, 17 December, <https://www.brighthorizons.com/article/employers/ai-workforce-readiness-crisis-79-of-workers-say-theyre-not-ready>
- Burke, R (2025) Unlocking Trends in the Cybersecurity Job Market, LinkedIn article, 2 December, <https://www.linkedin.com/pulse/unlocking-trends-cybersecurity-job-market-november-2025-ricki-burke-unvec/>
- Business Wire (2026) Survey Finds 45% of Cybersecurity Leaders Work a "Sixth Day" as AI Redefines Their Role, 4b March 2026, <https://finance.yahoo.com/news/survey-finds-45-cybersecurity-leaders-140000669.html>
- Comrise (2025) US White House AI report: Talent shortage exceeds 4 million, pp. 15-22, <https://comrise.com/news/u-s-white-house-ai-report-talent-shortage-exceeds-4-million/>
- Cyber Exchange UK (2025) DSIT publishes latest insights on UK cyber security skills in the UK labour market report, <https://cyberexchange.uk.net/news/dsit-publishes-latest-insights-on-uk-cyber-security-skills-in-the-uk-labour-market-report>
- Cybersecurity Guide (2026) Cybersecurity skills gap 2026: AI threats outpace workforce training. CybersecurityGuide.org. <https://cybersecurityguide.org/resources/cybersecurity-skills-gap/>
- CyberSkills2Work (2025) About the National Cybersecurity Workforce Development Program, <https://cyberskills2work.org/about/>

- Da Gama, M and Perucica, N (2025), AI is revolutionizing cybersecurity. How should we train professionals? World Economic Forum, 19 November, <https://www.weforum.org/stories/2025/11/cybersecurity-ai-professionals-workers/>
- Dawson R. (2020) 5 ambitious private sector initiatives preparing the workforce for a future of AI, <https://rossdawson.com/5-ambitious-private-sector-initiatives-preparing-the-workforce-for-a-future-of-ai/>
- e2 Cyber (2025) State of Cyber Security Job Market Australia: 2025 and Beyond, e2 Cyber, 5 August, <https://www.e2cyber.com.au/news/state-of-cyber-security-job-market-australia-2025-and-beyond>
- Eisenhower, DD (1957) Address at the National Defense Executive Reserve Conference, Washington DC, 14 November 1957, in *Public Papers of the Presidents of the United States: Dwight D. Eisenhower, 1957*. Washington DC: National Archives and Records Service, Government Printing Office, <https://www.presidency.ucsb.edu/documents/remarks-the-national-defense-executive-reserve-conference>
- FinTechWales (2026) Socura report highlights rapid growth in UK cyber security workforce, <https://fintechwales.org/news/socura-report-highlights-rapid-growth-in-uk-cyber-security-workforce/>
- Floridi L (2023) On the Brussels-Washington consensus about the legal definition of artificial intelligence, *Philosophy & Technology* 36 (4), <https://link.springer.com/article/10.1007/s13347-023-00690-z>
- Floridi L (2025) AI as Agency without Intelligence: On Artificial Intelligence as a New Form of Artificial Agency and the Multiple Realisability of Agency Thesis, *Philosophy and Technology*, 38, 30, <https://doi.org/10.1007/s13347-025-00858-9>
- Friedman S (2018) New MIT College of Computing to boost AI research across the institution, *Campus Technology*, 28 October, <https://campustechnology.com/articles/2018/10/29/new-mit-college-of-computing-to-boost-ai-research-across-the-institution.aspx>
- GIAC Certifications (2026) 2026 cybersecurity workforce study research reports: AI, regulation, and skills redefining careers and teams, GIAC. <https://www.giac.org/reports>
- Go1 (2026) AI training for employees: How to upskill your team in 2026, 31 March, <https://www.go1.com/blog/ai-training>
- Goh (2025) Securing Artificial Intelligence: Opportunities and Challenges, ISACA, <https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2025/volume-1/securing-artificial-intelligence-opportunities-and-challenges>
- Harvard University (n.d.) CS50's Introduction to Artificial Intelligence with Python, <https://pll.harvard.edu/course/cs50s-introduction-artificial-intelligence-python>
- Hollis M and Smith S (1991), *Explaining and understanding International Relations*, Clarendon, Oxford University Press, <https://www.scribd.com/document/355064005/Hollis-Martin-amp-Smith-Steve-Explaining-and-Understanding-International-Relations-pdf>
- Inside Higher Ed (2025) Google to Spend \$1B on AI Training in Higher Ed, <https://www.insidehighered.com/news/quick-takes/2025/08/07/google-spend-1b-ai-training-higher-ed>
- ISACA (2026) Taking the Pulse of AI in 2026, <https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/infographics/2026-taking-the-pulse-of-ai.pdf>
- ISACA (2025), 89% of Digital Trust Pros Say Increased AI Skills and Knowledge Needed to Retain Job or Advance Their Career Over Next Two Years, <https://www.isaca.org/about-us/newsroom/press-releases/2025/digital-trust-pros-say-increased-ai-skills-and-knowledge-needed-to-advance-their-career>

- ISC<sup>2</sup> (2024a) AI in Cyber 2024: Is the Cybersecurity Profession Ready?, <https://edge.sitecorecloud.io/internationalf173-xmc4e73-prod0f-9660/media/Project/ISC2/Main/Media/Marketing-Assets/Enterprise/ISC2-AI-Survey-Report.pdf>
- ISC<sup>2</sup> (2024b) Global Cybersecurity Workforce Prepares for an AI-Driven World ISC<sup>2</sup>, 2024 ISC<sup>2</sup> cybersecurity workforce study, <https://edu.arrow.com/media/wtjfm5zx/2024-isc2-wfs.pdf>
- ISC<sup>2</sup> (2025) 2025 ISC<sup>2</sup> cybersecurity workforce study: Cybersecurity Professionals Navigate Evolving Workplaces While Seizing New Opportunities, [https://edge.sitecorecloud.io/internationalf173-xmc4e73-prod0f-9660/media/Project/ISC2/Main/Media/insights/Features/2025/12/COMMS\\_2025\\_Cybersecurity\\_WFS\\_Report\\_Whitepaper.pdf](https://edge.sitecorecloud.io/internationalf173-xmc4e73-prod0f-9660/media/Project/ISC2/Main/Media/insights/Features/2025/12/COMMS_2025_Cybersecurity_WFS_Report_Whitepaper.pdf)
- Jepma W (2025) AI Impact on Cybersecurity Jobs in 2025, Cybercrime Magazine, 13 July, <https://solutionsreview.com/endpoint-security/what-will-the-ai-impact-on-cybersecurity-jobs-look-like-in-2025/>
- Jobs and Skills Australia (2025a) Jobs and Skills Report 2025, <https://www.jobsandskills.gov.au/publications/jobs-and-skills-report-2025>
- Jobs and Skills Australia (2025b) *Cyber security skills in demand as labour market evolves*, Australian Labour Market for Migrants – Hot Topic, <https://www.jobsandskills.gov.au/news/cyber-security-skills-demand-labour-market-evolves>
- Kitterman T. (2025) How the 100 Best Companies Are Training Their Workforce for AI, 31 January, <https://www.greatplacetowork.com/resources/blog/100-best-training-workforce-ai>
- Lee, V (2025) AI in Cybersecurity Job Market: Reshaping Careers in 2025, <https://airiam.com/blog/ai-in-cybersecurity-job-market/>
- Mervis J. (2018) MIT to use \$350 million gift to bolster computer sciences, Science, 14 October, <https://www.science.org/content/article/mit-use-350-million-gift-bolster-computer-sciences>
- Microsoft (2024) 'What is AI for cybersecurity?' Microsoft Security. Available at: <https://www.microsoft.com/en-us/security/business/security-101/what-is-ai-for-cybersecurity>
- Microsoft (2025) "Microsoft Digital Defense Report 2025 Lighting the path to a secure future" <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/bade/documents/products-and-services/en-us/security/Microsoft-Digital-Defense-Report-2025-v5-21Nov25.pdf>
- NIST (2025) "Cybersecurity Framework Profile for Artificial Intelligence (Cyber AI Profile)", (Draft), <https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8596.iprd.pdf>
- NSCAI (2021) Final Report: National Security Commission on Artificial Intelligence (AI), <https://apps.dtic.mil/sti/pdfs/AD1124333.pdf>
- Pasteur L (1854) Discours prononcé à Douai, le 7 décembre 1854, à l'occasion de l'installation solennelle de la Faculté des Lettres de Douai et de la Faculté des Sciences de Lille. Lille: University of Lille, <https://innovationetserendipite.wordpress.com/wp-content/uploads/2011/01/discours-de-louis-pasteur.pdf>
- Red Hat (2026) '4 use cases for AI in cyber security'. Red Hat Blog, <https://www.redhat.com/en/blog/4-use-cases-ai-cyber-security>
- Ross S (2025) Information Security Matters: Artificial Intelligence and Entry-Level Cybersecurity Jobs, *ISACA Journal*, vol. 5, <https://www.isaca.org/resources/isaca-journal/issues/2025/volume-5/artificial-intelligence-and-entry-level-cybersecurity-jobs>
- SANS (2026) SANS Research: The Cybersecurity Talent Shortage Narrative Is Wrong. The Real Crisis Is What Your Team Doesn't Know, Starting with AI,

- <https://www.sans.org/press/announcements/sans-research-cybersecurity-talent-shortage-narrative-wrong-real-crisis-what-your-team-doesnt-know-starting-ai>
- SANS GIAC (2025) 2026 Cybersecurity Workforce Research Report: The Evolving Cyber Workforce: AI, Compliance, and the Battle for Talent, <https://sansorg.egnyte.com/dl/mHPVHkTyxHY3>
- Scroton A (2026) 'Security now one of the UK's fastest-growing career paths', *Computer Weekly*, 28 January, <https://www.computerweekly.com/news/366637839/Security-now-one-of-the-UKs-fastest-growing-career-paths>
- Short L (2025) AI and the Future of Cyber Security: How Organizations and CISOs Can Prepare for AI-Driven Cyber Risks, Harvard Extension School Blog, 1 August, <https://extension.harvard.edu/blog/ai-and-the-future-of-cybersecurity/>
- Spencer S (2025), Key Trends in the 2025 London Cyber Security Job Market – Part 1, Barclay Simpson, 12 October, <https://www.barclaysimpson.com/key-trends-in-the-2025-london-cyber-security-job-market-part-1/>
- Stanford Institute for Human-Centered Artificial Intelligence (2025) Artificial Intelligence Index Report 2025 (Economy section), Stanford University, <https://hai.stanford.edu/ai-index/2025-ai-index-report/economy>
- Stanford Institute for Human-Centered Artificial Intelligence (2026) Artificial Intelligence Index Report 2026, [https://hai.stanford.edu/assets/files/ai\\_index\\_report\\_2026.pdf](https://hai.stanford.edu/assets/files/ai_index_report_2026.pdf)
- UK Cyber Security Council (2025) Keeping the UK focused on cyber security skills development in 2025, <https://www.ukcybersecuritycouncil.org.uk/blogs/keeping-the-uk-focused-on-cyber-security-skills-development-in-2025>
- UK. Department for Education & DSIT (2026) AI Skills for Life and Work: Summary report, <https://www.gov.uk/government/publications/ai-skills-for-life-and-work-summary-report/ai-skills-for-life-and-work-summary-report--2>
- UK. DSIT (2026) Cyber Security Sectoral Analysis, <https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2026/cyber-security-sectoral-analysis-2026>
- UK. DSIT (2024) Cyber security skills in the UK labour market 2024, <https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2024/cyber-security-skills-in-the-uk-labour-market-2024>
- UK. DSIT (2025a) Cyber security skills in the UK labour market 2025: findings report, Department for Science, Innovation and Technology, London, <https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2025>
- UK. DSIT (2025b) *Cyber security skills in the UK labour market 2025 and cyber security sectoral analysis 2025: technical report*, Department for Science, Innovation and Technology, London (authors: Jayesh Shah, Jamie Douglas, Alex Bollen, Sophia Hasapopoulos, Shahil Parmar, Grace Clarke, Sam Donaldson), [https://assets.publishing.service.gov.uk/media/6893291f303b0dad411d4e50/Cyber\\_security\\_skills\\_in\\_the\\_UK\\_labour\\_market\\_2025\\_-\\_technical\\_report.pdf](https://assets.publishing.service.gov.uk/media/6893291f303b0dad411d4e50/Cyber_security_skills_in_the_UK_labour_market_2025_-_technical_report.pdf)
- UK. DSIT (2025c) AI and Software Cyber Security Market Analysis, London, <https://www.gov.uk/government/publications/ai-and-software-cyber-security-market-analysis/ai-and-software-cyber-security-market-analysis>
- University of New Haven (n.d.) The NSA/NCAE-C Immersive Cybersecurity Workforce Development Program (ICWDP) <https://icwdp.newhaven.edu>
- US National Science Foundation (2026) NSF launches AI and cybersecurity education solicitation, enhancing longstanding Scholarship for Service program, 24 February, <https://www.nsf.gov/edu/updates/nsf-launches-ai-cybersecurity-education-solicitation>
- Wendt A (1987) 'The agent-structure problem in international relations theory', *International Organization*, 41(3), pp. 335–370, <https://www.rochelleterman.com/ir/sites/default/files/wendt%201987.pdf>

- Westover JH (2025) Enterprise AI Upskilling at Scale: Strategic Workforce Transformation in the Age of Generative AI, Human Capital Leadership Review, 20 October, <https://www.innovativehumancapital.com/article/enterprise-ai-upskilling-at-scale-strategic-workforce-transformation-in-the-age-of-generative-ai>
- Wetzel K (2025) The impact of artificial intelligence on the cybersecurity workforce, NIST, Online asset, <https://www.nist.gov/blogs/cybersecurity-insights/impact-artificial-intelligence-cybersecurity-workforce>
- White House (2023) National Cyber Workforce and Education Strategy, <https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf>
- White House (2025) Executive Order No. 14365, Ensuring a National Policy Framework for Artificial Intelligence, 11 December 2025, <https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/>
- Wight C (2006) *Agents, Structures and International Relations: Politics as Ontology*. Cambridge: Cambridge University Press, [https://api.pageplace.de/preview/DT0400.9780511247811\\_A23690573/preview-9780511247811\\_A23690573.pdf](https://api.pageplace.de/preview/DT0400.9780511247811_A23690573/preview-9780511247811_A23690573.pdf)
- Zwetsloot R with Heston R and Arnold Z (2019) Strengthening the US AI Workforce A Policy and Research Agenda, p. 4, [https://cset.georgetown.edu/wp-content/uploads/CSET\\_US\\_AI\\_Workforce.pdf](https://cset.georgetown.edu/wp-content/uploads/CSET_US_AI_Workforce.pdf)