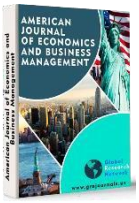

American Journal of Economics and Business Management

Vol. 8 Issue 11 | **pp.** 5343-5362 | **ISSN:** 2576-5973
Available online @ https://www.globalresearchnetwork.us/index.php/ajebm

Article

The Influence of AI, Technological Readiness, and Sectoral Differences on Talent Management: A Theoretical Review

Bian Jiang[1], Siti Hajar Mohamad[2], Angelina Anne Fernandez[3]

1. Graduate School of Management, Postgraduate Centre, Management and Science University, Shah Alam, 40100, Selangor, Malaysia
2,3 Department of Business Management and Law, Faculty of Business Management and Professional Studies, Management and Science University, Shah Alam, 40100, Selangor, Malaysia

Correspondence: [1]kvbian@gmail.com, [2]sitihajar_mohamad@msu.edu.my, [3]angelina_anne@msu.edu.my

Abstract: Beijing's financial, internet, and industrial industries have been among of the first to use aided, autonomous, and augmented AI to improve their cyber defences. Nonetheless, the ramifications of these technologies on local cybersecurity talent management are insufficiently examined, since current research mostly focusses on technological innovations rather than workforce evolution. The Diffusion of Innovations (DOI) theory elucidates sector-specific adoption trajectories, whereas the Skill-Biased Technological Change (SBTC) theory elucidates the emergence of skill premiums. To fill this gap, the current study looks at how the three AI modalities directly affect cybersecurity talent management, how organisational technological readiness acts as a mediator, and how industry characteristics in Beijing's corporate landscape act as a moderator. AI-based cybersecurity solutions have become increasingly popular since threats are harder to predict and more complex. The field will be affected by future developments in AI and cybersecurity. AI and cybersecurity will change the employment market and technology by creating demand for new occupations and skills. Self-healing networks, often known as autonomous security systems, are some of the most interesting new developments in cybersecurity. AI will find and get rid of cyber risks on its own, without any help from people. A self-healing network cuts off systems that have been attacked, repairs security holes, and restores safe settings without needing IT help.

Keywords: Assisted AI, Autonomous AI, Augmented AI, Cybersecurity Talent Management, Technological Readiness

Citation: Jiang B., Mohamad S. H. B., Fernandez A. A. The Influence of AI, Technological Readiness, and Sectoral Differences on Talent Management: A Theoretical Review. American Journal of Economics and Business Management 2025, 8(11), 5343-5362.

Received: 30th Sept 2025
Revised: 15th Oct 2025
Accepted: 25th Oct 2025
Published: 5th Nov 2025

1. Introduction

Innovation and application of AI, a disruptive technology, have become essential indicators of national strategic advantage (AlShebli et al., 2024). China's pursuit of AI implementation in this global setting has made it a major competitor to the US's hegemony, and both nations are driving the field in influence, newness, and human resources (AlShebli et al., 2024). This national strategic emphasis provides the macro-context needed to understand how AI affects particular sectors and talent ecosystems. China has committed to developing AI for an autonomous industrial foundation and extensive use of intelligent technology in the economy and society as a national strategy (Wang & Li, 2024). Due to advances in algorithms, processing power, and big data, Research found that China's AI business is growing fast through investment (Wang & Li, 2024). This top-down development model requires expansion in supporting industries, including cybersecurity.

The sophistication of cyber assaults has risen as Chinese society has integrated intelligent technology, necessitating expansion in the defence sector (Manoharan & Sarker, 2023).

Beijing is the main driver of national AI development, which has become one of the world's most powerful AIs. The city became the National AI Innovation and Development Pilot Zone. With careful implementation, the city promoted initiative growth. Industrial growth was forecast at $41 billion in November. Beijing developed the strongest ecosystem of 36 AI unicorns, achieving more than 50% of unicorns in China. Beijing's 46 AI listed companies had a market value of over 4.3 trillion RMB in the China A share market (Rui, 2024). Beijing leads the country in the latest wave of generative AI with roughly 94 big AI models, 40% of the national total (Rui, 2024). Beijing can examine AI adoption's effects in real time due to its capital, innovation, and enterprise concentration.

AI's rapid spread into banking, the internet, and industry in Beijing requires a deep grasp of cybersecurity. AI-driven assaults and cybersecurity automation provide significant problems. AI is helping cybercriminals create sophisticated phishing and deep-fake fraud attacks that outperform older technologies (Jimmy, 2021). AI protects systems defensively but risks adversarial assaults that circumvent system decision-making (Baniecki & Biecek, 2024). Inability to control cybersecurity risks drives Beijing organisations' Defence Cyber Operations to employ sophisticated AI technology. This diverse AI adoption demands understanding the balance of human control in aided, augmented, and autonomous AI systems. Integrating AI technology into Assisted AI means using AI as a strong tool to assist human analysts, who make the ultimate decision. AI can quickly analyse enormous amounts of data and give meaningful insights. AI anomaly detection analyses network data in real time to detect anomalous activity that may indicate a danger at a level that humans cannot attain manually (Goswami, 2024). Many well-documented AI applications give real-time situational awareness when humans make judgements. After retraining, malware detection AI models give Beijing's sophisticated internet and banking sector users real-time situational awareness to make swift judgements (Vasani et al., 2023).

Augmented AI shows a new level of human-AI collaboration. Augmented AI analyses alarms and reduces false positives to help analysts focus on complex, strategic concerns. Modern SR SOCs demonstrate this. Human analysts receive prioritised suggestions from an AI system that examines warnings and cross-references other data. After human analysts check, amend, or accept the AI idea, the system can handle more complicated occurrences. Human-in-the-loop design enhances cybersecurity system reaction quickness and operational effectiveness. The highest level of integration, autonomous AI, allows systems to make and execute choices within a strategic framework. These systems are essential for machine-speed threat response when human involvement is too slow. In automated incident response, AI bots may isolate devices and patch vulnerabilities to limit a breach without human intervention (Zhao et al., 2022). This change boosts operating efficiency and fortifies against assaults (Hassan & Ibrahim, 2023). Beijing's IT industry is dense and high-stakes, making real-time autonomous system action essential for cyber defence.

The explosive expansion of these three AI models is redefining cybersecurity and the industry workforce. Cybersecurity experts must develop new skills to work with AI systems (Michael et al., 2023). New hybrid workforce are needed to build, implement, and manage AI-driven security systems (Akhtar & Rawol, 2024). New 'AI Security Engineer' roles integrate machine learning and high-level threat analysis (Rangaraju, 2023). Cybersecurity experts' roles are changing. They must comprehend system security, AI model findings, bias, and vulnerability assessment. Modern cybersecurity people managers face the complicated twin dilemma of sufficient, relevant skills and recruiting as AI-driven systems proliferate. Beijing organisations must build answers to sophisticated, AI-based risks using the above competencies.

An organization's competitive edge in the digital age depends on the use of new technology. Technology Readiness Level (TRL) is a popular paradigm for assessing an organization's capacity to grow a technology's maturity from inception to commercialisation (Mankins, 2009). The TRL paradigm is important but inadequate in fast-changing areas like cybersecurity, where technical innovation is rapid. Adopting advanced technologies like AI depends on "organisational readiness" as much as technological maturity. Current studies assess the more complex "organisational digital transformation readiness" by considering not only technological tools and infrastructure but also the organization's strategy, operational processes, culture, and most importantly, people's "organisational readiness" (Silva et al., 2025; Michelotto & Joia, 2024). Even the most sophisticated AI technology will not be useful if an organisation has poorly structured internal procedures to govern and unassisted individuals to run, analyse, and oversee it. A complete analysis of an organization's preparation across sectors would reveal AI's effects on cybersecurity talent management. Beijing has banking, internet, and manufacturing businesses, so preparation may be compared. Different industries' importance and variety provide a unique opportunity.

The high-readiness industries are simpler than Beijing's manufacturing industry, which has diverse technical readiness. The city participates in China's national "AI + Manufacturing" strategy plan for intelligent technology-driven industrial upgrades, although factory conditions are still complicated and heterogeneous (Interesse, 2025). Many national programs, such as "Made in China 2025", have advanced industrial digitalisation by creating around 8,000 digital workshops and smart factories (China Briefing, 2025). Progressive manufacturers embrace new technologies. However, separating Traditional Operational Technology (OT) from contemporary IT is difficult. Many Beijing manufacturing plants have outdated ICS and SCADA systems. Those systems regulate physical processes but lack current internet connectivity and cyber-security, making integration with modern AI systems unfeasible (De Azambuja et al., 2023).

Technological and talent dilemmas coexist. Connecting contemporary production requires specialised understanding. The ideal applicant will have extensive industrial engineering, OT protocols, current IT, cloud computing, and AI security experience. There aren't enough university graduates in both professions to produce a sustained stream of expert problem-solvers. Beijing's manufacturing enterprises face a technical gap in their fundamental infrastructure and a shortage of OT-IT professionals. It goes beyond recruiting more cybersecurity experts. This change requires a new class of professionals to assure safety. In conclusion, industry AI preparedness varies. Manufacturing has fundamental integration challenges, while finance and internet face governance issues. Despite their differences, many businesses confront the same challenge: enough human expertise is the fundamental limiting factor for highly successful AI application to cybersecurity. The following part will examine the human resources gap between ambitions and realities. Previous parts have described Beijing's tech scene: a policy-supported AI growth and an opaque and unequal technical maturity band in its essential industries. However, both of these are part of a big technological revolution that raises difficult concerns about a company's most valuable asset: its personnel. AI in cybersecurity alters jobs, skills, and security teams. Thus, industrial AI thinking should focus on talent management rather than the "job market," because talent management is more tactical and strategic. This section reviews the research to outline four facets of this problem for talent acquisition, development, workforce planning and organisational design, and retention. These characteristics illustrate the AI cybersecurity human capital dilemma.

Companies face a critical talent acquisition dilemma due to the massive gap between rising demand and a shortage of trained workers. The global scarcity of skilled professionals is well-known and longstanding. The need for qualified defenders has increased as cyberattacks have gotten more sophisticated (Liu et al., 2020). Global

shortages of competent professionals have resulted from insufficient supply to satisfy rising demand (Blažič, 2021). UNCTAD estimated that 3.4 million competent cybersecurity jobs were open worldwide in 2024, and this figure is rising. Companies compete for the same talented people in a competitive labour market. In a bustling, dynamic city like Beijing, where most enterprises and businesses are digital, this talent battle puts a lot of pressure on recruiting.

Changes in demand increase the talent acquisition dilemma. There is a lack of cybersecurity specialists and people with hybrid abilities to work in an AI setting (Morandini et al., 2023; Khan, 2024). Instead of network analysts or penetration testers, companies are looking for someone who can bridge the gap between traditional security abilities and AI (George, 2024). This creates a "two-body problem": traditional security professionals lack the AI and data science knowledge to address new threats, and AI specialists lack the operational skills and knowledge to operate in a cybersecurity environment (Ricci et al., 2024). The difficulty of recruiting and valuing people with these skills increases hiring costs and time. Modern cybersecurity teams must purposefully locate, recruit, and integrate these unique, multi-disciplinary talent pools (Pacheco, 2025). Companies must develop innovative ways to uncover these related skill sets and transcend their standard recruitment methods.

To fill skill gaps, firms are “upskilling” and “reskilling” current employees due to the challenges and costs of attracting external expertise. Current employees know they need corporate learning programs to close the skills gap. In China, 81.3% of cybersecurity specialists said they needed AI training to keep ahead (Ministry of Industry and Information Technology Education and Examination Centre et al. 2024). How can firms create learning programs to bridge employee skills gaps? This concern is twofold: upskilling, which involves adding to an employee's current skills to improve their performance in their current role with new AI tools, and reskilling, which involves learning new skills for a new role created by automation and AI (Oladimeji Egon & Broklyn 2024).

Strategy and structure are needed to create effective upskilling and reskilling strategies. The World Economic Forum (2024) recommends a talent strategy framework that helps businesses predict future skill shortages and build development routes. Academic consensus is growing that AI integration both a technology problem and a key HRD issue. A rigorous review shows that AI and automation are transforming HRD theory and practise (Ekuma, 2024). Therefore, HRD theory and practise in businesses must change to lifelong learning models (Ekuma, 2024). A conceptual framework that links AI technology adoption with comprehensive HRD programmes is needed to use AI for sustainable businesses (Yawson & Goryunova, 2025). Only less than a third of universities worldwide offer specialised AI security courses, so employers must ‘build their own talent pipelines’ to build a future-ready workforce (UNCTAD, 2024).

At the intersection of AI and cybersecurity, new, highly specialised occupations are emerging in addition to automation. “AI Security Engineers” safeguard and construct AI systems, “Adversarial Machine Learning Specialists” attack and defend them, and “AI Ethics and Compliance Consultants” assure ethical AI usage and data privacy compliance (George, 2024). New occupations like “AI Red Team Experts” and “Deepfake Detection Specialists” will keep coming (Baseri, Chouhan, & Hafid, 2024). Very important for organisation design and structure. Due to increased job creation, security teams may need to be more integrated, with data scientists, security analysts, and software engineers working together.

Overall, the literature is poor and sparse. The disruptive impact of AI on cybersecurity positions has been recognised, but strategic organisational talent management approaches have not been addressed. It recognises technology readiness and industry variations as moderators but has not included them in an explanatory model. This

study seeks to fill an obvious, important, and testable gap in the literature: the moderated mediation mechanism via which AI technology deployment affects cybersecurity talent management practices. It is unclear how organisational technological preparedness mediates this link and how industry factors temper the mediation process. This study develops and tests a model that incorporates these variables to provide a meaningful, theory-based explanation of the complex relationship between technology, organisational capability, and human capital strategy in the AI era. According to the issue description, this study examines how AI affects cybersecurity skills.

Literature Review

Skill-Biased Technological Change

The well-established Skill-Biased Technological Change (SBTC) theory was used in this study to explain how technological change—assisted, augmented, and autonomous AI—affects the cybersecurity workforce's composition and skill requirements. SBTC theory claims that technological development favours higher-skilled labour. The theory states that new technologies increase productivity and demand for higher-skilled workers who can perform non-routine tasks and produce goods and services, while replacing and devaluing routine, codifiable workers (Kiley, 1999). The total effect alters earnings and employment in affected industries. our skill-biased shift is driven by all three AI types in our research. With SBTC theory, this research may go beyond characterising AI in the cybersecurity workforce to systematically studying its implications on organisational talent management.

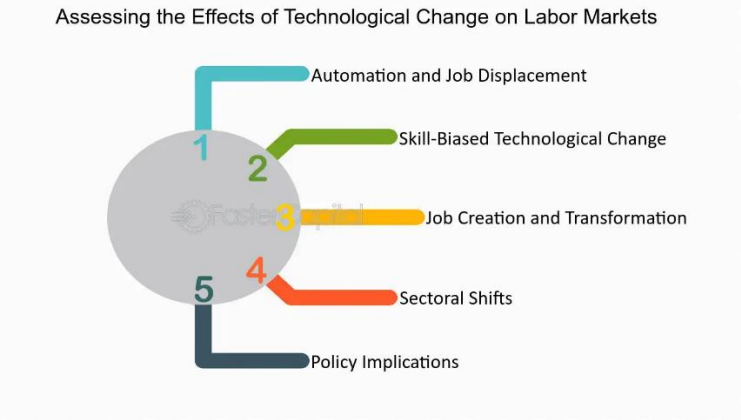

Figure 1. Skill-Biased Technological Change (SBTC) theory. (Faster capital. Retrieved, 2025).

SBTC operates mostly by reassigning jobs around an organisation. Autor, Levy, and Murnane (2003) found that computerisation replaces routine physical and mental work and complements abstract work. Applying this to cybersecurity, AI technology will quickly cause this substitution impact. Assisted and autonomous AI will automate time-consuming tasks like log monitoring, preliminary alarm triage, and basic vulnerability screening (Autor, Levy, & Murnane, 2003). Automation is why you need AI; autonomous AI can uncover aberrant network data sets better than humans and is essential to security operations (Graham, 2025). This substitution impact will change workforce planning and organisational design. When regular work is mechanised, its value decreases, and organisations restructure positions and teams. As Autor, Katz, and Kearney (2006) found in the broader labour market, the security workforce may be "polarised" as demand focusses on high-skilled analysts and low-skilled IT support, while mid-band, routine monitoring is hollowed out.

The more powerful skill complementarity method is now available together with task substitution. Since the AI handles security, it frees up more and preferably better-trained personnel to handle response. Human analysts will be creative, analyse complex problems, devise and implement strategies, and they will complement AI, not replace it, because, as in the example above, the analyst does the heavy lifting, puts the threat in the context of the organization's risk posture, and develops the response strategy. AI only enables the latter (Dave, Mandvikar, & Engineer, 2023). The effects on talent acquisition and competence modelling are huge. Modelling the standard security skills inventory is insufficient. Technology increases labour complexity and demand for workers, according to Acemoglu and Autor (2011). This might be a machine learning engineer developing autonomous AI code or a data scientist interpreting its outputs in cybersecurity.

Task substitution and skill complementarity generate a large gap between worker capabilities and industrial demands. SBTC theory makes the strongest case for prioritising talent development (upskilling and reskilling) in modern talent management. Acemoglu and Restrepo (2018) define automation as having a "displacement effect" that eliminates low-skill employment and a "productivity effect" that creates high-skill jobs. Proactively addressing the skills gap is necessary to navigate this transformation. It's commonly known that market-ready talent with autonomous AI capabilities like machine learning for anomaly detection is scarce (Graham, 2025). Due to this shortage, organisations must establish their own talent pipelines through focused internal training. SBTC theory emphasises the necessity for continual learning and workforce development to prepare people for a quickly changing job market (Graham, 2025).

The present AI innovation surge is more complicated than SBTC says. Modern automation can drive “upstream innovation” that makes existing tasks and processes more efficient, but augmented AI is also creating “horizontal innovation” in cybersecurity, new capabilities that didn't exist before. These create need for new cybersecurity positions like “AI-Driven Threat Analyst” and “Threat Intelligence Specialist” (Hémous & Olsen, 2022; Graham, 2025). Change is faster and more dramatic. ISC2 (2024) found that AI technologies are affecting 88% of cybersecurity professions. This rapid direct effect shows that SBTC-predicted cybersecurity workforce shifts are happening faster than expected (Graham, 2025). In such a world, contextual elements (which we shall investigate using DOI theory in the following section) will be important. Whether a firm is ‘technology-ready’—meaning it has the right infrastructure and skills—may alter the entire process. Companies with strong computational capabilities and skilled people are better able to apply AI and feel the full impact of skill-biased transformation, resulting in quicker job creation and role conversion (Acemoglu and Autor, 2011). AI implementation may be slower in less tech-savvy organisations, delaying worker effect (Acemoglu & Restrepo, 2018). Industry characteristics also moderate. Competitive markets speed up AI adoption, increasing need for high skills (Hémous and Olsen, 2022), and legal limits in finance boost demand for high skills.

Table 1. Theoretical Review Table About Skill-Biased Technological Change.

Author & Year	Title	Area	Variables	Findings
Autor, Levy, & Murnane (2003)	The Skill Content of Recent Technological Change: An Empirical Exploration	Labor Economics	Computer technology, skill demands, task types, organizational readiness	Computer technologies like AI and autonomous AI shift cybersecurity tasks toward high-skill activities (e.g., threat analysis),

				increasing demand for roles like data scientists. Organizational readiness, such as AI training programs, mediates adoption, enabling firms to integrate AI and reshape the job market.
Autor, Katz, & Kearney (2006)	The Polarization of the U.S. Labor Market	Labor Economics	Technology, high/low-skill jobs, industry structure	AI-driven technologies polarize the cybersecurity talent management, boosting high-skill roles (e.g., AI security analysts) while automating routine tasks. Industry characteristics, such as competitive markets, accelerate AI adoption, driving demand for high-skill professionals.
Acemoglu & Autor (2011)	Skills, Tasks and Technologies: Implications for Employment and Earnings	Labor Economics	Technology, skills/tasks, organizational capabilities	AI technologies (e.g., autonomous AI, augmented AI) increase demand for high-skill cybersecurity tasks (e.g., algorithm design). Technological readiness, such as system upgrades, mediates adoption, fostering job growth in AI-driven firms and redefining workforce needs.
Acemoglu & Restrepo (2018)	The Race Between Man and Machine: Implications of Technology	Automation and Labor	Automation/AI, employment outcomes, technological readiness,	AI and automation, including autonomous AI, enhance cybersecurity

		for Growth, Factor Shares, and Employment		industry regulations	efficiency, creating high-skill jobs (e.g., threat detection experts). Technological readiness (e.g., AI infrastructure) mediates job creation, while industry regulations (e.g., compliance requirements) moderate adoption speed, shaping workforce transformation.
	Hémous & Olsen (2022)	The Rise of the Machines: Automation, Horizontal Innovation, and Income Inequality	Automation and Inequality	AI/automation, skill bias, industry competition	AI technologies like augmented AI drive skill-biased demand in cybersecurity, increasing roles for AI-skilled professionals (e.g., machine learning engineers). Competitive industry environments accelerate AI adoption, amplifying job market changes and emphasizing high-skill expertise.
	Graham, C.M. (2025)	AI Skills in Cybersecurity: Global Job Trends Analysis	Cybersecurity and AI Skills	AI skills, cybersecurity job demands, technological readiness, regional industry variations	AI skills, such as machine learning and neural networks for autonomous AI, are in high demand globally for roles like threat intelligence analysts. Technological readiness (e.g., upskilling programs) mediates skill adoption, while industry

				characteristics (e.g., regional policies in USA/UK) moderate demand, boosting AI-specialist roles.
ISC2 (2024)	2024 ISC2 Cybersecurity Workforce Study	Cybersecurity Workforce	AI technologies, workforce roles, technological readiness, cyber threat landscape	AI technologies, including autonomous AI for threat monitoring, impact 88% of cybersecurity roles, creating high-skill positions like AI-driven threat analysts. Technological readiness (e.g., AI tool integration) mediates role transformation, while rising cyber threats (industry characteristics) drive demand for AI-skilled professionals.

In conclusion, the Skill-Biased Technological Change theory represents the primary theoretical lens through which to understand the fundamental drivers behind one of the key study outcomes. This goes beyond simply observing technological change to explaining why and how technological change occurs and how it impacts the workforce. Through explaining the drivers of task substitution and skill complementarity, SBTC explains the fundamental drivers of modern cybersecurity talent management: the need for robust workforce planning to manage role reclassification, the need for the development and implementation of new competency standards in talent acquisition and the need for continuous upskilling and reskilling in talent development. While other theories will be used to explain how this change occurs in practice, SBTC provides the theoretical foundation through which to understand the ultimate impact on the cybersecurity human capital's structure, skills and management.

Diffusion of Innovations

While Skill-Biased Technological Change (SBTC) theory explains for the final consequences of technological change on the workforce, this study needs another theory to explain how, why, and how quickly technology evolves inside an organisation. This study relies on Rogers (1962)'s Diffusion of Innovations (DOI) hypothesis. According to DOI theory, new ideas and technologies (an "innovation") travel across a social system at a certain rate. In this paradigm, AI adoption in cybersecurity is modelled as a process impacted by the technology, the organisation adopting it, and the industrial context in which it works. DOI theory focusses on five innovation traits that might influence an organization's adoption: relative advantage, compatibility, complexity, trialability, and observability (Rogers, 1962). This research justified aided, enhanced, and autonomous AI IVs with these properties. These AI technologies are the "innovations" spreading in

cybersecurity. Adoption is driven by their advantage over traditional security measures. Autonomous AI's capacity to identify complex network breaches in seconds boosts speed and efficacy (Syu et al., 2025) and attracts technologically savvy enterprises. The degree to which an invention fits an organization's beliefs, historical experiences, and resources, including cybersecurity infrastructure, is also crucial. An AI solution that needs a major overhaul of an organization's SOC is less likely to be accepted than one that can be simply incorporated. However, the intricacy of an innovation—how much work it takes to use it—can hinder its acceptance. Advanced augmented AI requires specialised workers and large infrastructure, slowing its adoption (Haefner et al., 2021). In the digital age, GitHub and other open-source projects accelerate trialability (the ability to use an innovation on a limited basis) and observability (the visibility of an innovation's results), allowing firms to see the benefits of an innovation, such as fewer successful cyberattacks, before fully adopting it (Rogers, 2003).

DOI theory goes further to explain that not all social system members accept innovations. Based on their inherent “innovativeness” and other traits, adopters might be innovators, early adopters, early majority, late majority, and laggards. This reasoning theoretically supports our study's Mediating Variable (MV): Tech Ready. Our study defines the "adopter" as the organisation, and its technological readiness is the operationalisation of individual adopter traits. An “innovator” or “early adopter” in Rogers' classification is a technologically ready organisation with advanced infrastructure, workforce, and culture that encourages it. These organisations are most likely to trial and succeed with new AI security tools. Moore (1991) highlighted a “chasm” between imaginative early adopters and the pragmatic early majority in his high-tech market books. Organisational technology preparedness closes the chasm. For instance, a mainstream organisation with modern cloud infrastructure and qualified AI security experts may embrace and grow augmented and autonomous AI technologies and alter its workforce. However, if it lacks preparedness, it might hinder or prohibit adoption and its influence on talent management. Technological readiness is much more than a contextual factor—it mediates how and to what extent an organisation can realise the promise of an AI invention.

Finally, DOI theory states that diffusion occurs in a "social system," whose norms, structure, and communication channels influence innovation adoption figure 2. our social structure theoretically justifies Industry Characteristics as the Moderating Variable in our study. Industry shapes an organization's AI perspectives, pressures, and possibilities. Research supports this idea from several sources. Valente (1996) discovered that network architectures and opinion leaders affect industry competition and cooperation. When one firm's AI adoption (opinion leader) succeeds, like in the internet business, other firms may follow suit to stay competitive (Moore, 1991; Hémous & Olsen, 2022). Khan et al. (2024) also noted that industry regulation and risk moderate systems. Geopolitical threats and overbearing government laws might slow AI adoption. High-handed banking laws encourage AI use for compliance and fraud detection. However, ethical issues and possible abuse in data-rich situations can hinder and restrict AI technology adoption (Syu et al., 2025). Industry communication framework is crucial. Close professional networks and a culture of collaboration speed innovation and best practice spread, whereas siloed industries delay it (Valente, 1996). Thus, industry factors may moderate the link between an organization's technical readiness and its personnel management methods to adapt to AI.

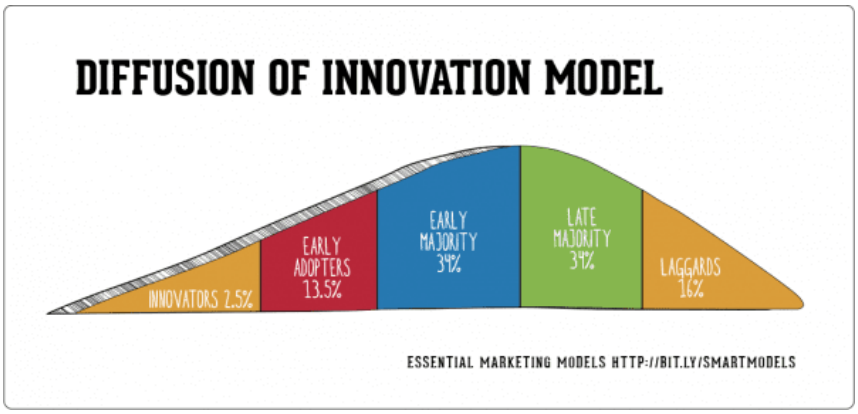

Figure 2. DOI theory. Hanlon (2013).

Table 2. Theoretical Review Table About Diffusion of Innovations.

Author & Year	Title	Area	Variables	Findings
Rogers, E. M. (1962)	Diffusion of Innovations	General DOI Theory	Innovation attributes (relative advantage, compatibility, complexity, trialability, observability), adopter categories (innovators, early adopters, early majority, late majority, laggards)	Innovation attributes like relative advantage (e.g., AI's efficiency in threat detection) and compatibility (e.g., integration with cybersecurity systems) drive adoption speed. Adopter categories influence AI diffusion, with innovators and early adopters (e.g., tech-forward firms) leading adoption, shaping technological readiness.
Moore, G. A. (1991)	Crossing the Chasm	High-tech Markets	Innovation attributes (relative advantage, compatibility, complexity), adopter categories (early adopters, early majority), technological readiness	AI technologies (e.g., autonomous AI, augmented AI) with high relative advantage (e.g., efficient threat detection) and compatibility are adopted faster in network security firms. A chasm between early adopters and early majority is mediated by technological readiness (e.g.,

				infrastructure readiness), impacting AI diffusion.
	Valente, T. W. (1996)	Network Models of the Diffusion of Innovations	General DOI Theory	Social network structure, opinion leaders, industry characteristics	Opinion leaders in cybersecurity firms (e.g., tech influencers) drive AI adoption (e.g., augmented AI) through dense industry networks. Industry characteristics (e.g., competitive pressure) moderate diffusion speed, with networked firms showing higher technological readiness for AI integration.
	Rogers, E. M. (2003)	Diffusion of Innovations (5th ed.)	Internet-based Innovations	Digital communication channels, social networks, innovation attributes (relative advantage, trialability), technological readiness, industry characteristics	Digital channels (e.g., tech forums, GitHub) accelerate AI diffusion in cybersecurity by enhancing trialability. Social networks and industry characteristics (e.g., regulatory frameworks) shape technological readiness, enabling faster adoption of AI tools like autonomous AI in compliant firms.
	Haefner, N., et al. (2021)	Artificial Intelligence and Innovation Management: A Review, Framework, and Research Agenda	AI and Innovation Management	AI as innovation (relative advantage, complexity), technological readiness (organizational preparedness), industry characteristics (industry structure)	AI's relative advantage (e.g., automation in cybersecurity) drives adoption, but complexity (e.g., augmented AI implementation) requires high technological readiness (e.g., training, infrastructure).

				Industry characteristics (e.g., competitive intensity) accelerate diffusion in innovative sectors.
Khan, K., et al. (2024)	Is Artificial Intelligence a New Battleground for Cybersecurity?	AI in Cybersecurity	AI technology (relative advantage, compatibility), technological readiness (defensive capabilities), industry characteristics (geopolitical risks, regulations)	AI's relative advantage (e.g., rapid anomaly detection in autonomous AI) enhances cybersecurity adoption, but geopolitical risks and regulations (industry characteristics) slow diffusion. Technological readiness (e.g., upgraded defense systems) mediates AI's impact on security practices.
Syu, J.-H., et al. (2025)	AI-driven Fusion with Cybersecurity: Exploring Current Trends, Advanced Techniques, Future Directions, and Policy Implications	AI-driven Cybersecurity	AI technologies (autonomous AI, augmented AI: relative advantage, complexity), technological readiness (system integration), industry characteristics (policy, ethics), cybersecurity talent management (skills demand)	autonomous AI and augmented AI's relative advantage (e.g., adaptive threat detection) improves cybersecurity efficiency, but high complexity demands robust technological readiness (e.g., system upgrades). Industry characteristics (e.g., ethical policies) moderate adoption, while AI diffusion increases demand for AI-skilled professionals, reshaping the cybersecurity talent management.

In summary, the Diffusion of Innovations theory offers a comprehensive and robust blueprint for modeling the AI adoption process and its expected impact on organizations. This study can thus transcend a superficial input-output model and examine a series of events. By aligning the core tenets of DOI theory onto the study's research framework, this

study's theoretical argument is clear: the Innovations (three forms of AI) are adopted by organizations through the Adopter Characteristics (Technological Readiness) and this occurs within the context of the Social System (Industry Characteristics). This process-oriented view, combined with the outcome-oriented view offered by SBTC theory, enables this study to comprehensively explore how AI is reshaping the cybersecurity workforce.

2. Discussion

Synthesizing the Theories to Build the Research Framework

The previous sections have reviewed the strengths of Skill-Biased Technological Change (SBTC) and Diffusion of Innovations (DOI) theory in explaining the cybersecurity workforce trend, but a more holistic understanding of AI's role in shaping the cybersecurity talent landscape requires a more concerted integration of the two theories. Both theories offer limited insights when used in isolation: SBTC theory describes what happens with skill demands and job tasks after a technology is implemented, but it is largely silent on how and why organisations fail to adopt (or adopt) a technology. DOI theory describes how and why organisations adopt a technology, but it does not specify the skill-biased human capital consequences. A dual-lens theory is needed to link the introduction of an AI breakthrough to its effects on talent management practices. This study claims that DOI and SBTC theories are complimentary since each describes one sequential portion of the research model. The integrated approach allows a more detailed examination, linking organizational-level technology adoption to team- and individual-level work and skill improvements.

First, this paper employs DOI theory to outline AI acceptance and deployment. It links AI technology availability to organisational transformation. This study defines the research model's major constructs. Assisting, augmenting, and autonomous AI are "Innovations" whose perceived features (e.g., relative advantage, complexity) impact acceptance. The core set of "Adopter Characteristics" at the organisational level is the Mediating Variable (Technological Readiness), which measures the firm's internal competence and innovativeness to absorb and execute AI advancements. Last, the Moderating Variable (Industry Characteristics) is the diffusion "Social System". The regulatory pressures, competitive dynamics, and technology standards of the financial, Internet, and industrial sectors may impact the dissemination process. DOI hypothesis explains the IVs, MV, and Moderator connections.

SBTC theory complements this process-oriented approach by interpreting the eventual effects of technological adoption on the organization's human capital. Successful AI acceptance and deployment, the DOI process's conclusion, feeds SBTC's predictions. SBTC's task substitution and skill complementarity effect cybersecurity work. This article uses theory to explain why Cybersecurity Talent Management is the study's dependent variable. The automation of regular labour and rising need for sophisticated, non-routine analytical tasks generate workforce planning, talent acquisition and upskilling, and organisational design issues. This study uses SBTC as the crucial theoretical lens to justify the dependent variable and anticipate its future changes.

This integrated framework, which connects the process of AI adoption with its outcomes on talent management. Threat detection automation may be the greatest cybersecurity advance (Okoli et al., 2024). Antivirus software used pre-programmed malware signatures. Rule-based software only blocked threats it had been configured to identify. With AI-based anomaly detection, cyber defence systems can now identify known and undiscovered risks like zero-day assaults by detecting strange and inconsistent data and behaviour patterns. This move has had two effects on employment. AI systems may detect hazards without human intervention, reducing the requirement for manual surveillance. Unfortunately, it has created new jobs for AI trainers, who teach AI systems

to detect new dangers, and false-positive analysts, who analyse and improve AI models to decrease mistakes (Nagar, 2018).

Another technical breakthrough is enhanced AI in security operations. AI is used to enhance human decision-making, not replace it. SOAR platforms combine AI and human skills in cybersecurity. These technologies automate incident triage and response but leave risk assessment and strategy to specialists. It has transformed the workforce, creating hybrid professions with technical and interpretative skills. Incident handlers who previously processed security issues manually now help AI systems track and understand AI-generated alerts to make contextual and firm-specific decisions (Moencks et al., 2022). Generative AI changed cyberattacks and defences. AI helps cyber security experts, but it also helps cyber attackers. GPT-based generative AI systems have created sophisticated phishing campaigns and malware code (Hasanov et al., 2024). Adversarial AI specialists have emerged from this two-way AI use in cybersecurity. AI defence and cybercrime countermeasures are the specialities of these professionals. Generative AI in cybersecurity has created new labour market niches where experts must keep ahead of the curve with AI-driven protection mechanisms and AI-based cyberattacks. Economic reasons have driven cybersecurity AI use. Large-scale cybersecurity assaults can cost organisations a lot in breach remediation, legal fines, reputation harm, and customer loss. As cyberattacks become more costly, firms must improve their cybersecurity to prevent losses (Moore, 2010).

AI can monitor networks for suspicious activity, scan vulnerabilities, and detect malware, making it an inexpensive security method. Businesses may save costs, identify dangers faster, and eliminate errors by replacing human labour with AI. AI-powered cybersecurity solutions can improve threat detection with fewer false positives and less intervention, making them a good investment for organisations that want more protection without breaking the bank (Prince et al., 2024). With automation expansion, AI should reduce breach remediation costs and improve operational efficiency even further. Regulatory reforms and compliance requirements have also driven cybersecurity tech innovation. In recent years, governments have imposed stricter data protection rules, such as the EU's General Data Protection Regulation (GDPR) and the NIST AI Risk Management Framework. These guarantee organisations securely store personal and sensitive data. AI technologies are increasingly used to automate compliance activities and ensure cybersecurity compliance (Marotta & Madnick, 2021). AI may monitor and invoke data protection mechanisms, identify breaches, and evaluate security measures to assure privacy compliance. The rising requirement for AI-compliance solutions shows AI's growing relevance in addressing today's complicated cybersecurity standards. AI will become increasingly important in helping organisations comply with data protection and privacy laws as they change.

Another reason for the need for AI-based solutions is the fast-changing cyber threat scenario. Zero-day attacks, APTs, and AI-driven attacks are becoming more common amidst sophisticated cyber threats. Traditional rule-based security technologies that employ pre-configured signatures may miss these new threats. To identify and eliminate such dynamic dangers, machine learning (ML) and behaviour analytics are essential. AI-based systems can analyse massive amounts of data in real time to discover harmful behaviour that may suggest an attack. As new threats emerge, machine learning algorithms can improve these systems' detection (Liu & Lang, 2019). AI has become a crucial weapon for countering cyberattacks since they have gotten more complex and unpredictable, hence cybersecurity solutions that use AI have increased. AI and cybersecurity developments will affect the sector in the future. The trends will have a huge influence on technology and the labour market because AI and cybersecurity will increase demand for new occupations and skills. Self-healing networks, or autonomous security systems, are one of the most exciting cybersecurity innovations. These AI-powered systems will detect and eliminate cyber threats without human interaction (Ko, 2020). A

self-healing network will isolate compromised systems, correct vulnerabilities, and restore safe configurations without IT intervention when it detects an assault.

Self-healing networks would speed up incident response and help organisations recover from cyberattacks or minimise damage. Self-healing security systems will likely grow more complex and effective at addressing additional cyber-attacks as AI capabilities improve. Such systems might signal a shift from reactive to proactive, self-healing cybersecurity. AI and automation in cybersecurity have revolutionised monotonous processes like log analysis, malware analysis, and vulnerability detection. More precise and efficient technology might eliminate the need for human interaction in many processes, according to studies. This move does not usually reduce cybersecurity specialists (Brynjolfsson & McAfee, 2014). Instead, it seems to spur new activity in domains that require specialists in AI settings and interpretation, offering entry opportunities for AI and cybersecurity experts. Strategic positions involving technical and interpretative abilities are becoming more important as AI is integrated into cybersecurity operations (Dahlman & Westphal, 2019). Emerging positions include cyber risk managers, AI security architects, and AI ethicists. AI security architects architect AI-enabled systems, whereas cyber risk managers analyse and mitigate cybersecurity risk. The rise of AI ethicists, who address transparency and ethical technology usage, has raised concerns about AI adoption in cybersecurity (Vemuri, Thaneeru, & Tatikonda, 2023). These trends suggest profession-wide skill needs.

Technology advances quickly, requiring cybersecurity experts to continue their education. Access to new AI technology and approaches increases the need for constant upskilling to ensure worker flexibility. AI, machine learning, and other advanced cyber defence training programs are called for by experts to meet market demands. Well-prepared technologically—defined by such training—organizations are better equipped to accept newer technologies, demonstrating a link between technology integration and skill improvement (Pradhan & Saxena, 2023).

3. Conclusion

This study creates a strong, unified theoretical framework by combining the Diffusion of Innovations (DOI) theory and the Skill-Biased Technological Change (SBTC) theory. This dual-lens approach is essential for a comprehensive analysis of AI's impact on the cybersecurity workforce, as either hypothesis alone is inadequate. The framework sequentially connects the process of adopting new technology in an organisation to the results for its employees. DOI theory offers the fundamental framework, elucidating how the perceived features of helping, augmenting, and autonomous AI affect organisational adoption, mediated by technology preparedness and modulated by industry traits. The results of this adoption process then set off the main ideas of SBTC theory, which describes what happens next: the reorganisation of cybersecurity talent management. SBTC explains how AI automates everyday jobs while also generating a need for complex, non-routine analytical abilities. This makes workforce planning, upskilling, and organisational design very difficult.

The practical consequences of this concept are clear in the changing world of cybersecurity. The rise of AI-powered technologies, including SOAR platforms, anomaly detection, and generative AI, is not just a replacement for work; it is a change in work. As a result, manual, regular jobs have become less common, and new hybrid and highly specialised jobs have appeared, such as AI trainers, false-positive analysers, adversarial AI specialists, and AI ethicists. The economic pressure, regulatory compliance, and a more complex threat landscape that are pushing AI adoption are also directly causing a structural change in the job market. The cybersecurity expert of the future will need both technical abilities and the ability to think strategically and understand information. This integrated DOI-SBTC framework offers a holistic perspective to foresee, examine, and manage the intricate relationship between technological advancement and the developing

cybersecurity talent ecosystem, emphasising that the incorporation of AI presents both organisational and human capital challenges, in addition to technical ones.

REFERENCES

Abdallah, W., Harraf, A., & Al Wael, H. (2025). Factors influencing artificial intelligence implementation in the accounting industry: A comparative study among private and public sectors. Journal of Financial Reporting and Accounting. https://doi.org/10.1108/JFRA-04-2024-0230

Ahmed, S. A. A. S., & Isak, M. A. (2024). Factors affect cyber security readiness and performance of SMEs: A case study of Mogadishu, Somalia. International Journal of Innovative Science and Research Technology, 9(7), 1059–1069. https://doi.org/10.38124/ijisrt/IJISRT24JUL264

Akhtar, M., Salman, A., Ghafoor, K. A., & Kamran, M. (2024). Artificial intelligence, financial services knowledge, government support, and user innovativeness: Exploring the moderated-mediated path to fintech adoption. Heliyon, 10(21). https://doi.org/10.1016/j.heliyon.2024.e39521

Alharahsheh, H. H., & Pius, A. (2020). A review of key paradigms: Positivism vs interpretivism. Global Academic Journal of Humanities and Social Sciences, 2(3), 39–43. https://doi.org/10.36348/gajhss.2020.v02i03.001

Ali, I. M. (2024). A guide for positivist research paradigm: From philosophy to methodology. Idealogy Journal, 9(2), 187–196. https://doi.org/10.24191/idealogy.v9i2.596

Andress, J., & Winterfeld, S. (2013). Cyber warfare: Techniques, tactics and tools for security practitioners. Elsevier.

Arefin, S., & Simcox, M. (2024). AI-driven solutions for safeguarding healthcare data: Innovations in cybersecurity. International Business Research, 17(6), 1-74. https://doi.org/10.5539/ibr.v17n6p74

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333

Autor, D. H., Levy, F., & Murnane, R. J. (2003). The skill content of recent technological change: An empirical exploration. The Quarterly Journal of Economics, 118(4), 1279-1333. https://doi.org/10.1162/003355303322552801

Becher, T., & Torka, S. (2024). Exploring AI-enabled cybersecurity frameworks: Deep-learning techniques, GPU support, and future enhancements. arXiv preprint. https://doi.org/10.48550/arXiv.2412.12648

Benias, N., & Markopoulos, A. P. (2017, September). A review on the readiness level and cyber-security challenges in Industry 4.0. In 2017 South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM) (pp. 1-5). IEEE. https://doi.org/10.23919/SEEDA-CECNSM.2017.8088234

Bhardwaj, A. K., Dutta, P. K., & Chintale, P. (2024). AI-powered anomaly detection for Kubernetes security: A systematic approach to identifying threats. Babylonian Journal of Machine Learning, 2024, 142-148. https://doi.org/10.58496/BJML/2024/014

Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2022). Cybersecurity supply chain risk management practices for systems and organizations. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161r1

Charmet, F., Tanuwidjaja, H. C., Ayoubi, S., Gimenez, P. F., Han, Y., Jmila, H., & Zhang, Z. (2022). Explainable artificial intelligence for cybersecurity: A literature survey. Annals of Telecommunications, 77(11), 789–812. https://doi.org/10.1007/s12243-022-00926-7

Chauhan, P., Yadav, R. K., & Simon, R. (2024). Decoding AI's impact on the workforce: A comprehensive analysis of opportunities, challenges, and strategic adaptations in job markets. Global Journal of Enterprise Information System, 16(2), 40–47. https://gjeis.com/index.php/GJEIS/article/view/780

Dave, D. M., Mandvikar, S., & Engineer, P. A. (2023). Augmented intelligence: Human-AI collaboration in the era of digital transformation. International Journal of Engineering Applied Sciences & Technology, 8(6), 24-33. http://www.ijeast.com

Dave, D. M., Mandvikar, S., & Engineer, P. A. (2023). Augmented intelligence: Human-AI collaboration in the era of digital transformation. International Journal of Engineering Applied Sciences & Technology, 8(6), 24-33. http://www.ijeast.com

Dopamu, O., Adesiyan, J., & Oke, F. (2024). Artificial intelligence and US financial institutions: Review of AI-assisted regulatory compliance for cybersecurity. World Journal of Advanced Research and Reviews, 21(3), 964-979. https://doi.org/10.30574/wjarr.2024.21.3.0791

Ee, S., O'Brien, J., Williams, Z., El-Dakhakhni, A., Aird, M., & Lintz, A. (2024). Adapting cybersecurity frameworks to manage frontier AI risks: A defense-in-depth approach. arXiv preprint. https://doi.org/10.48550/arXiv.2408.07933

Folorunso, A., Adewumi, T., Adewa, A., Okonkwo, R., & Olawumi, T. N. (2024). Impact of AI on cybersecurity and security compliance. Global Journal of Engineering and Technology Advances, 21(1), 167–184. https://doi.org/10.30574/gjeta.2024.21.1.0193

Gadde, H. (2023). AI-driven anomaly detection in NoSQL databases for enhanced security. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 14(1), 497–522. https://ijmlrcai.com/index.php/Journal/index

Geluvaraj, B., Satwik, P. M., & Ashok Kumar, T. A. (2019). The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. In International Conference on Computer Networks and Communication Technologies: ICCNCT 2018 (pp. 739–747). Springer Singapore. https://doi.org/10.1007/978-981-10-8681-6_67

Graham, C. M. (2025). AI skills in cybersecurity: Global job trends analysis. Information & Computer Security. https://doi.org/10.1108/ICS-09-2024-0235

Graham, C. M., & Lu, Y. (2023). Skills expectations in cybersecurity: Semantic network analysis of job advertisements. Journal of Computer Information Systems, 63(4), 937–949. https://doi.org/10.1080/08874417.2022.2115954

Hajjar, S. T. (2018). Statistical analysis: Internal-consistency reliability and construct validity. International Journal of Quantitative and Qualitative Research Methods, 6(1), 27–38.

Hémous, D., & Olsen, M. (2022). The rise of the machines: Automation, horizontal innovation, and income inequality. American Economic Journal: Macroeconomics, 14(1), 179-223. https://doi.org/10.1257/mac.20160164

Jabbarova, K. (2023). AI and cybersecurity—new threats and opportunities. Journal of Research Administration, 5(2), 5955–5966. https://orcid.org/0009-0009-5797-0968

Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cybersecurity: An outcome of a systematic literature review. Data and Information Management, 8(2), 100063. https://doi.org/10.1016/j.dim.2023.100063

Jayaraman, S., Talib, P., & Khan, A. F. (2018). Integrated talent management scale: Construction and initial validation. SAGE Open, 8(3), 2158244018780965. https://doi.org/10.1177/2158244018780965

Kaminski, J. (2011). Diffusion of innovation theory. Canadian Journal of Nursing Informatics, 6(2), 1-6. https://tinyurl.com/y6zwh6l5

Kiley, M. T. (1999). The supply of skilled labour and skill-biased technological progress. The Economic Journal, 109(458), 708-724. https://doi.org/10.1111/1468-0297.00470

Kim, H., & Shon, T. (2022). Industrial network-based behavioral anomaly detection in AI-enabled smart manufacturing. The Journal of Supercomputing, 78(11), 13554–13563. https://doi.org/10.1007/s11227-022-04408-4

Ko, R. K. (2020). Cyber autonomy: Automating the hacker–self-healing, self-adaptive, automatic cyber defense systems and their impact on industry, society, and national security. In Emerging technologies and international security (pp. 173–191). Routledge.

Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. Applied Sciences, 9(20), 4396. https://doi.org/10.3390/app9204396

Liu, X., Xie, L., Wang, Y., Zou, J., Xiong, J., Ying, Z., & Vasilakos, A. V. (2020). Privacy and security issues in deep learning: A survey. IEEE Access, 9, 4566-4593. https://doi.org/10.1109/ACCESS.2020.3045078

Mankins, J. C. (2009). Technology readiness assessments: A retrospective. Acta Astronautica, 65(9-10), 1216-1223. https://doi.org/10.1016/j.actaastro.2009.03.058

Mankins, J. C. (2009). Technology readiness assessments: A retrospective. Acta Astronautica, 65(9–10), 1216–1223. https://doi.org/10.1016/j.actaastro.2009.03.058

Manoharan, A., & Sarker, M. (2023). Revolutionizing cybersecurity: Unleashing the power of artificial intelligence and machine learning for next-generation threat detection. IRJMETS, 1. https://doi.org/10.56726/IRJMETS32644

Michelotto, F., & Joia, L. A. (2024). Organizational digital transformation readiness: An exploratory investigation. Journal of Theoretical and Applied Electronic Commerce Research, 19(4), 3283-3304. https://doi.org/10.3390/jtaer19040159

Mohan, V., & Othmane, L. B. (2016). SecDevOps: Is it a marketing buzzword? Mapping research on security in DevOps. 2016 11th International Conference on Availability, Reliability and Security (ARES), 542-547. https://doi.org/10.1109/ARES.2016.92

Moore, G. A. (1991). Crossing the chasm: Marketing and selling high-tech products to mainstream customers. HarperBusiness.

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection, 3(3-4), 103–117. https://doi.org/10.1016/j.ijcip.2010.10.002

Nagar, G. (2018). Leveraging artificial intelligence to automate and enhance security operations: Balancing efficiency and human oversight. Valley International Journal Digital Library, 78-94. https://doi.org/10.18535/ijsrm/v6i7.ec05

Njenga, K., & Matemane, B. (2025). Augmented intelligence in social engineering attacks: A diffusion of innovation perspective. International Journal of Business Ecosystem & Strategy, 7(1), 106–121. https://doi.org/10.36096/iibes.v7i1.676

Nowrozy, R. (2024, July). GPTs or grim position threats? The potential impacts of large language models on non-managerial jobs and certifications in cybersecurity. Informatics, 11(3), 45. MDPI. https://doi.org/10.3390/informatics11030045

Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. World Journal of Advanced Research and Reviews, 21(1), 2286–2295. https://doi.org/10.30574/wjarr.2024.21.1.0315

Oladimeji, S., Egon, A., & Broklyn, P. (2024). Cybersecurity workforce development: Bridging the skills gap in the age of automation. Available at SSRN. https://ssrn.com/abstract=4904939 or http://dx.doi.org/10.2139/ssrn.4904939

Pillai, R., Sivathanu, B., Mariani, M., Rana, N. P., Yang, B., & Dwivedi, Y. K. (2022). Adoption of AI-empowered industrial robots in auto component manufacturing companies. Production Planning & Control, 33(16), 1517-1533. https://doi.org/10.1080/09537287.2021.1882689

Ramezan, C. A. (2023). Examining the cyber skills gap: An analysis of cybersecurity positions by sub-field. Journal of Information Systems Education, 34(1), 94-105. https://aisel.aisnet.org/jise/vol34/iss1/8

Rangaraju, S. (2023). Secure by intelligence: Enhancing products with AI-driven security measures. EPH-International Journal of Science And Engineering, 9(3), 36-41. https://doi.org/10.53555/ephijse.v9i3.212

Roshanaei, M., Khan, M. R., & Sylvester, N. N. (2024). Enhancing cybersecurity through AI and ML: Strategies, challenges, and future directions. Journal of Information Security, 15(3), 320–339. https://doi.org/10.4236/jis.2024.153019

Schmitt, M. (2023). Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. arXiv preprint. https://doi.org/10.48550/arXiv.2401.01342

Shahana, A., Hasan, R., Farabi, S. F., Akter, J., Mahmud, M. A. A., Johora, F. T., & Suzer, G. (2024). AI-driven cybersecurity: Balancing advancements and safeguards. Journal of Computer Science and Technology Studies, 6(2), 76–85. https://doi.org/10.32996/jcsts

Sills, M., Ranade, P., & Mittal, S. (2020, November). Cybersecurity threat intelligence augmentation and embedding improvement-a healthcare usecase. In 2020 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 1-6). IEEE. https://doi.org/10.1109/ISI49825.2020.9280482

Stockemer, D. (2019). Quantitative methods for the social sciences: A practical introduction with examples in SPSS and Stata (1st ed.). Springer International Publishing. https://doi.org/10.1007/978-3-319-99118-4

Uren, V., & Edwards, J. S. (2023). Technology readiness and the organizational journey towards AI adoption: An empirical study. International Journal of Information Management, 68, 102588. https://doi.org/10.1016/j.ijinfomgt.2022.102588

Uren, V., & Edwards, J. S. (2023). Technology readiness and the organizational journey towards AI adoption: An empirical study. International Journal of Information Management, 68, Article 102588. https://doi.org/10.1016/j.ijinfomgt.2022.102588

Valente, T. W. (1996). Network models of the diffusion of innovations.

World Economic Forum. (2024). Strategic cybersecurity talent framework. Retrieved from https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf

Yaseen, A. (2023). AI-driven threat detection and response: A paradigm shift in cybersecurity. International Journal of Information and Cybersecurity, 7(12), 25–43. https://orcid.org/0009-0002-8950-0767

Yau, K. L. A., Lee, H. J., Chong, Y. W., Ling, M. H., Syed, A. R., Wu, C., & Goh, H. G. (2021). Augmented intelligence: Surveys of literature and expert opinion to understand relations between human intelligence and artificial intelligence. IEEE Access, 9, 136744-136761. https://doi.org/10.1109/ACCESS.2021.3115494

Yawson, R. M., & Goryunova, E. (2025). Nested complexity: A conceptual framework for leveraging AI for sustainable organizations and human resource development. Advances in Developing Human Resources. https://doi.org/10.1177/15234223251335908

Zeng, H., Yunis, M., Khalil, A., & Mirza, N. (2024). Towards a conceptual framework for AI-driven anomaly detection in smart city IoT networks for enhanced cybersecurity. Journal of Innovation & Knowledge, 9(4), 100601. https://doi.org/10.1016/j.jik.2024.100601

Zhiyan Research. (2024). 2024-2030 China AI security industry market panoramic survey and development prospect analysis report. Retrieved from https://www.chyxx.com/research/1180119.html

Zhou, L., Pan, S., Wang, J., & Vasilakos, A. V. (2017). Machine learning on big data: Opportunities and challenges. Neurocomputing, 237, 350–361. https://doi.org/10.1016/j.neucom.2017.01.026