AI Readiness in National Cybersecurity Strategies: A Cross-Country Comparative Study

Chukwuemeka Ezekwem[1*]; Chidiebere Ucheji[2]; Justin Ekeneme[3]

[1]University of Chester

[2,3]Teesside University

***Corresponding Author**

DOI: https://doi.org/10.51584/IJRIAS.2025.1010000067

Received: 04 October 2025; Accepted: 10 October 2025; Published: 06 November 2025

ABSTRACT

The increasing integration of artificial intelligence (AI) into cybersecurity has reshaped national security strategies worldwide. This study investigates AI readiness in national cybersecurity strategies through a comparative analysis of three distinct governance models: the United States, China, and the European Union (represented by France). Using a systemic document review methodology, the research provides a comparative, cross-country analysis of AI readiness within national cybersecurity strategies. The results reveal three divergent strategic approaches to AI readiness: a public-private, market-driven ecosystem in the United States that fosters rapid innovation but can lead to fragmented national strategy; a top-down, state-led approach in China that enables rapid resource mobilisation and large-scale data collection at the potential cost of individual liberties; and a regulation-first framework in the European Union that prioritises ethical integrity and public trust. The analysis further found that a nation's economic maturity and human capital are foundational to its capacity for AI readiness, regardless of its governance model. The discussion highlights a fundamental trade-off between the speed of innovation and ethical oversight, arguing that an effective national strategy must be holistic and adaptive, combining policy guidance with targeted investment in technology, talent, and international collaboration.

Keywords: AI readiness, cybersecurity, national strategies, United States, China, European Union, Comparative analysis, governance models.

INTRODUCTION

Cybersecurity is a collection of tools, procedures, and methods used to prevent attacks, damage, and illegal access to networks, devices, software, and data (Perwej et al., 2021). The notion of "AI readiness" in national cybersecurity strategies refers to a state where strategic documents not only acknowledge the risks and benefits of AI but also systematically embed institutional, technical, regulatory, and capacity mechanisms to anticipate, prevent, detect, respond to, and recover from AI-enabled cyber threats. AI readiness encompasses dimensions such as governance frameworks specific to AI security, institutional coordination, human capital and skills, research and development, data infrastructure, threat intelligence sharing, and regulatory oversight (Ajani et al., 2025; Al Dajeh, 2024; Isagah and Dhaou, 2024).

The increasing integration of artificial intelligence (AI) into various sectors of society has created a new paradigm for national security, particularly in the domain of cybersecurity (Kaur et al., 2024). AI's capacity for rapid data analysis, pattern recognition, and autonomous decision-making presents both a powerful tool for defence and a potent weapon for malicious actors (Adewale, 2025). Nations are grappling with a dual challenge: leveraging AI to enhance their cybersecurity postures while simultaneously defending against AI-driven threats (Khan et al., 2025). There have been attempts to use AI technology to anticipate and identify different types of cyberattacks. For over ten years, the security sector has been using AI to develop a system that analyses, disseminates, and defends attack information to withstand changes in attackers (LG CNS, 2016). But ten years ago, harmful intrusions were less varied than they are now. As a result, efforts to use AI technology for cybersecurity have gotten little attention.

Furthermore, the intrusion detection and attack analysis system was able to completely protect against these attacks thanks to the pattern matching technique. However, the modern cyber risks brought on by cybersecurity problems are significant in both number and breadth compared to the scenario ten years ago (Yoo, 2017). There will probably be an even greater rise in these assaults. Because new information and communications technology (ICT) businesses are constantly emerging, cyberattacks have gotten more sophisticated, well-organised, and varied, making them more successful than in the past. To properly respond to this development in cyber-attacks, a variety of technological and administrative solutions and response systems have become increasingly required. People have also asked how cyberattacks react and whether it's feasible to predict how they will change every day. Or can unexpected Black Swans—which, once they happen, seriously harm systems—be identified and addressed beforehand? The necessity of using AI technology, which is expected to offer solutions to these queries, has just come to light (LG CNS, 2016).

Machine learning (ML) is one of the most often used terms to characterise AI applications in cybersecurity and is a key component of the upcoming cybersecurity defensive frontier (Perlman, 2019). Security control, threat detection, and prevention are just a few of the cybersecurity domains where ML technology is being used in research and applications. Additionally, it offers a prompt, potent, and proactive real-time reaction to cyberthreats (Kumar, 2019). Cybersecurity is made easier, more proactive, and more efficient by these security services (Perlman, 2019). Three broad categories may be used to group these safe machine learning problems and solutions. The primary applications of this technique are in problem solving, including decision trees, regression, diagnostics, classification, and recognition. The technique is applied in the realm of cybersecurity for virus detection, spam filtering, and network traffic analysis. Second, unsupervised learning is a method of learning just by posing problems. It is most effective when it comes to finding features and is mostly utilised for clustering for network anomaly detection, malware identification, and user behaviour analytics. Third, learning by evaluating results is known as reinforcement learning. By using this technique, ML agents can acquire behaviour through encounters in environments that resemble games (Bommelaer et al., 2017).

Despite the policy salience of AI in cybersecurity, comparative academic work remains sparse. Many existing national cybersecurity strategy assessments mention AI among emerging technologies (Kharbanda et al., 2023) but do not systematically evaluate how deeply AI is integrated into policy instruments. This study aims to provide a comprehensive cross-country comparative analysis of AI readiness within national cybersecurity strategies. By examining a diverse set of countries, this paper seeks to identify key commonalities and divergences in their strategic approaches. The findings are relevant for cyber policymakers, international development agencies, and scholars of AI governance and cybersecurity.

METHODOLOGY

This study employs a systematic documentative review methodology to analyse and compare national strategic approaches to the intersection of Artificial Intelligence (AI) and cybersecurity. This approach allows for a deep, contextual understanding of the policies and frameworks adopted by different nations, moving beyond simple data aggregation to a nuanced analysis of strategic intent, priorities, and implementation models. The study selected a purposive sample of countries representing diverse geopolitical, economic, and technological landscapes. The samples include 1) a major technological power with a market-driven approach (United States), 2) a state with a centralised, government-led strategy (China), and 3) a regional bloc with a strong regulatory focus (European Union, using a representative member state as a case study). This selection allows for the examination of distinct policy models and their impact on AI readiness.

Sources and Search Strategy

The primary sources for this review were official government documents, including AI national strategies, cybersecurity strategies, policy white papers, and legislative texts. To ensure a comprehensive search, the following keywords and phrases were used in various combinations across official government websites, think tank publications, and academic databases (e.g., Google Scholar, Scopus, Web of Science, IEEE Xplore, and

PubMed): using keywords such as "AI readiness", "national cybersecurity strategy", "artificial intelligence AND cybersecurity policy", and "comparative cybersecurity strategies". The search was restricted to English-language documents but included countries from diverse regions to maximise comparability.

Eligibility Criteria

The documents were screened for inclusion based on the following criteria:

- **Inclusion Criteria:** Documents are widely recognised reports from reputable international organisations or government publications directly addressing the national strategy for AI and/or cybersecurity. The documents are published between 2015 and 2025 to ensure relevance and currency. Also, documents had to be available in English.
- **Exclusion Criteria:** Documents were excluded if they were journalistic articles, opinion pieces, or preliminary drafts not formally adopted as policy. Documents that focused solely on general technology policy without explicit mention of AI and cybersecurity were also excluded.

Study Selection

The selection process followed a two-stage approach. In the first stage, the titles and abstracts of the retrieved documents were screened for relevance against the eligibility criteria. This initial screening was conducted by the researcher to quickly identify a broad set of potentially relevant sources. In the second stage, a full-text review of the selected documents was performed to confirm their relevance and extract key data points related to the study. Any uncertainties during the selection process were resolved through discussion.

Quality Assessment

The quality and reliability of each source were assessed to mitigate bias and ensure the validity of the findings. The primary quality metric was the document's official status, with official government white papers and legislative acts being given the highest weight. Reports from independent and well-regarded think tanks were also considered highly reliable. Documents were also evaluated based on the clarity of their methodology and the presence of empirical evidence to support their claims. This ensured that the analysis was based on the most authoritative and credible sources available.

RESULTS

The cross-country comparison revealed significant variations in AI readiness across the selected cases—the United States, China, and the European Union (represented by France)—largely driven by differing strategic priorities and governance models. These differences manifest in technological capability, threat perception, and the ethical and legal frameworks governing AI development and deployment.

The United States: A Public-Private Ecosystem

In the United States, AI readiness is primarily propelled by a dynamic public-private ecosystem, a model built on decentralised innovation and market-driven incentives. The government's role is often that of a catalyst and facilitator, fostering innovation through substantial grants and research programmes (Dimitriadis, 2025). A prime example is the Defence Advanced Research Projects Agency (DARPA), which has historically funded foundational AI research that later finds its way into commercial applications, from autonomous systems to natural language processing (Ledbetter, 2022; U.S. Department of War, 2025). This approach has led to a highly innovative environment where technological capability is extremely high, with a global concentration of leading AI and cybersecurity firms.

This decentralised model, however, also presents challenges. The lack of a single, overarching national strategy can lead to a fragmented approach to AI adoption and governance (Themann, 2025). While the Department of Defence (DoD) might have advanced AI initiatives, a civilian agency's readiness may lag. This fragmentation can also create gaps in national cybersecurity posture, as different sectors—from finance to energy—develop their own security protocols with varying degrees of maturity (Clapp, 2025). Threats are often in terms of great-power competition and the protection of intellectual property and critical infrastructure from foreign adversaries, as articulated in documents like the National AI Initiative Act of 2020. The emphasis on intellectual property protection is a direct reflection of the private sector's dominance in AI R&D, with government policy serving to safeguard these investments (White & Case 2024).

Consequently, this public-private dynamic has yielded an ecosystem where innovation is rapid, but regulation is often reactive. The development of AI-driven cybersecurity tools is largely in the hands of private companies, with the government, while agile, sometimes prioritising commercial viability over robust, comprehensive security standards, creating a tension between speed and safety.

China: A State-Led, Top-Down Approach

China presents a stark contrast with its top-down, state-led strategy, as outlined in its "Next Generation Artificial Intelligence Development Plan" 2017 (Wong et al., 2024). The government has designated AI as a national priority, with extensive state funding and policy directives aimed at achieving global leadership in the field by 2030 (Roberts et al., 2019). This centralised control allows for the rapid mobilisation of resources and large-scale data collection, which is crucial for training complex AI models. China's ability to mandate data sharing across sectors and build massive, centralised data lakes gives it a significant advantage in areas like computer vision and natural language processing (Peredy et al., 2022). As a result, China shows a high degree of integration of AI into its national security apparatus, particularly in areas of surveillance, defence and social governance.

The use of AI for public safety, urban management, and predictive policing is a key component of its national strategy (Raji and Sholademi, 2024). This model, however, raises significant ethical and privacy concerns, as the collection and use of citizen data are subject to state control rather than individual consent (Pina et al., 2024). The threat perception is heavily focused on maintaining internal stability and countering external influence, with AI technologies being viewed as critical tools for social control and national defence (Gilbert and Gilbert, 2024). The state's top-down approach allows for rapid deployment of AI-driven cybersecurity systems at a national scale, but it also means that the same systems can be used to monitor and control citizens (Mary, 2025).

Ultimately, it has been shown that this model prioritises collective national goals over individual rights, which fundamentally shapes the nature of its AI readiness. While it achieves remarkable speed and scale, the lack of independent oversight and public debate on ethical implications means that the development path is highly controlled and less responsive to external criticism.

The European Union: A Regulation-First Model

The European Union, represented here by a nation like France, exhibits a regulation-first approach to AI readiness. The model is best exemplified by the EU AI Act, which focuses on managing the risks associated with AI by categorising applications based on their level of risk and setting stringent requirements for high-risk systems (Gstrein et al., 2024). For instance, AI systems used in critical infrastructure or law enforcement face the most rigorous standards, including mandatory human oversight and data governance (Cate, 2025). Additionally, technical development is strong, especially in countries like France and Germany with robust research institutions and engineering talent; the pace of adoption can be slower due to compliance burdens (Skare and Soriano, 2021). Public-private partnerships are encouraged, but within a highly structured and regulated environment where data privacy (enforced by GDPR) and ethical guidelines are paramount (Pina et al., 2024).

The threat perception in the EU is often rooted in protecting democratic values and citizen data privacy, with a focus on preventing AI from being used to manipulate public discourse or infringe upon fundamental rights (Cupać and Sienknecht, 2024). Thus, this approach contrasts sharply with the US model's market-driven focus and China's state-led control, placing the EU as a global leader in the ethical governance of AI. While this may slow down commercialisation, it aims to build public trust and ensure AI is developed and used in a way that aligns with democratic principles (Jørgensen and Ma, 2025). Hence, the focus is not just on technological capability but on responsible technology capability.

DISCUSSION

The findings from this cross-country comparison reveal that AI readiness is not a monolithic concept but a multifaceted outcome shaped by district national governance models and strategic priorities. The results underscore a fundamental trade-off between speed of innovation and safety and ethical oversight, with each nation's chosen model reflecting its core values and perceived national interest. While the United States' decentralised, market-driven approach has fostered rapid technological advancement, it has also led to a fragmented national strategy (Themann, 2025). Conversely, China's state-led, top-down model enables remarkable speed and scale at the potential cost of individual liberties (Peredy et al., 2022). The European Union's regulation-first framework, in turn, prioritises ethical integrity and public trust, which may slow down adoption but aims to create a more sustainable and equitable AI ecosystem (Balcioğlu et al., 2025).

The central tension identified in this result is the divergence in how nations approach the governance of technological power. In line with research by Polyakov et al. (2024), the U.S. model, rooted in a tradition of private sector innovation, views government primarily as an enabler and a customer. This system is highly effective at fostering groundbreaking research and development and is unparalleled in its ability to commercialise new technologies. However, the lack of a unified, comprehensive national strategy can create critical gaps in cybersecurity posture, leaving various sectors vulnerable to attacks (Adegbite et al., 2023). Thus, the threat perception is external and economic, focusing on intellectual property theft and great-power competition.

In contrast, China's model demonstrates the immense power of a centralised, state-led approach. The government's ability to direct resources and mobilise a massive workforce towards a single national objective—global AI leadership—is a significant strategic advantage. In line with the works of Zou and Zhang (2025) and Roberts et al. (2020), this centralised control facilitates the rapid and large-scale deployment of AI systems, particularly for internal security and social governance. The primary threat perception is internal, centred on maintaining stability and controlling information. This model, while efficient, presents a fundamental challenge to global norms on privacy and human rights, leading to a significant ethical debate on the responsible use of AI.

The European Union's approach offers a third, distinct pathway. By prioritising a human-centric, regulation-first framework, the EU seeks to set a global standard for the responsible development of AI (Arora et al., 2025; Yazici, 2025). The EU AI Act is a landmark effort to mitigate risks and ensure that AI systems are trustworthy and accountable. This focus on regulatory integrity, however, introduces a different kind of trade-off (European Parliament, 2025). While it builds public trust and may lead to more robust, ethical systems, the compliance burdens can slow the pace of innovation and adoption compared to the more agile U.S. and Chinese models. On the other hand, the EU's threat perception is uniquely focused on protecting democratic values and citizen data privacy from both state and corporate overreach.

Ultimately, the analysis reveals that a nation's AI readiness is not simply a function of its governance model but is deeply intertwined with its underlying economic and social foundations. The findings highlight that regardless of whether a country is market-led, state-led, or regulation-first, a strong economic base foundational element—significant GDP, R&D investment, and a skilled workforce—is the primary determinant of a nation's capacity to develop and implement sophisticated AI technologies. This suggests that the global AI landscape is likely to see a divergence of these three distinct models, creating a competitive environment where each system's strengths and weaknesses will be tested in real time

RECOMMENDATIONS

Based on this comparative analysis, the following recommendations are proposed for nations seeking to enhance their AI readiness in cybersecurity:

1. Nations should move beyond treating AI as a mere technological tool and instead integrate it as a central pillar of their national cybersecurity strategy. This strategy should clearly define roles for government, industry, and academia and outline a vision for leveraging AI for both defensive and offensive cyber capabilities.

2. A nation's greatest asset in the AI era is its people. Hence, governments should invest in robust educational programmes to create a pipeline of AI and cybersecurity professionals. This includes fostering STEM education from an early age, supporting advanced university research, and implementing reskilling initiatives for the current workforce.
3. Government cannot address the AI-cyber challenge alone. They must actively partner with the private sector, which often holds the most advanced AI technology and talent. This can be achieved through an environment that incentivises innovation while ensuring security.
4. While regulation is necessary, an overly restrictive approach can stifle innovation. Nations should consider a risk-based framework like the EU's, where high-risk AI applications are subject to strict oversight, while low-risk applications are given more freedom to innovate.
5. Given the global nature of cyber threats, no country can be truly secure in isolation. Nations must actively participate in international forums, share best practices, and work together to establish global norms and standards for the ethical and responsible use of AI in cybersecurity. This includes collaboration on AI-driven threat intelligence sharing and joint vulnerability research.

CONCLUSION

This cross-country comparative study demonstrates that AI readiness in national cybersecurity is a complex, multi-dimensional issue. It is not simply a matter of technological prowess but is deeply influenced by a nation's governance model, strategic priorities, and human capital. While the United States, China, and the European Union represent distinct approaches, their experiences offer valuable lessons for all nations. A comprehensive and effective strategy for AI readiness in cybersecurity must be holistic, combining clear policy guidance with targeted investments in technology, talent, and international collaboration. Moving forward, the race for AI dominance in cybersecurity will not be won by the country with the most advanced technology alone, but by the one with the most intelligent and adaptive strategy.

REFERENCES

1. Adegbite, A.O., Akinwolemiwa, D.I., Uwaoma, P.U., Kaggwa, S., Akindote, O.J. and Dawodu, S.O. (2023). Review of cybersecurity strategies in protecting national infrastructure: Perspectives from the USA. Computer Science & IT Research Journal, 4(3), pp.200–219. doi:https://doi.org/10.51594/csitrj.v4i3.658.
2. Adewale, T. (2025). AI-driven cyberattacks and defence tactics: A critical analysis of adversarial threats in modern security systems. ResearchGate. Available at: https://www.researchgate.net/publication/390746598_AI-Driven_Cyber_Attacks_and_Defense_Tactics_A_Critical_Analysis_of_Adversarial_Threats_in_Modern_Security_Systems [Accessed 28 Apr. 2025].
3. Ajani, H.A., Yusuf, O., Muogbo, C. and Mustapha, B. (2025). AI readiness framework for African businesses: Assessing capabilities and gaps. ResearchGate. doi:https://doi.org/10.13140/RG.2.2.22355.90406.
4. Al Dajeh, B.M. (2024). Artificial intelligence governance. Journal of Ecohumanism, 3(4), pp.300–313. doi:https://doi.org/10.62754/joe.v3i4.3515.
5. Arora, A.S., Saboia, L., Arora, A. and McIntyre, J.R. (2025). Human-centric versus state-driven. International Journal of Intelligent Information Technologies, 21(1), pp.1–13. doi:https://doi.org/10.4018/ijiit.367471.
6. Balcioğlu, Y.S., Çelik, A.A. and Altindağ, E. (2025). A turning point in AI: Europe's human-centric approach to technology regulation. Journal of Responsible Technology, p.100128. doi:https://doi.org/10.1016/j.jrt.2025.100128.
7. Bommelaer, C., et al. (2017). Artificial intelligence and machine learning: Policy paper. Internet Society. Available at: https://www.internetsociety.org/resources/doc/2017/artificialintelligence-and-machine-learning-policy-paper/
8. Cate, M. (2025). Global regulatory frameworks and their stance on AI in compliance.
9. Clapp, S. (2025). Defence and artificial intelligence. European Parliament. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf.

10. Cupać, J. and Sienknecht, M. (2024). Regulate against the machine: How the EU mitigates AI harm to democracy. Democratization, 31(5), pp.1–24. doi:https://doi.org/10.1080/13510347.2024.2353706.
11. Dimitriadis, D. (2025). US vs EU AI plans – A comparative analysis of the US and European approaches. Available at: https://dcnglobal.net/posts/blog/us-vs-eu-ai-plans-a-comparative-analysis-of-the-us-and-european-approaches [Accessed 5 Aug. 2025].
12. European Parliament (2025). EU AI Act: First regulation on artificial intelligence. Available at: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.
13. Gilbert, C. and Gilbert, M.A. (2024). The impact of AI on cybersecurity defense mechanisms: Future trends and challenges. Global Scientific Journal, 12(9), pp.427–441. doi:https://doi.org/10.11216/gsj.2024.09.229721.
14. Gstrein, O.J., Haleem, N. and Zwitter, A. (2024). General-purpose AI regulation and the European Union AI Act. Internet Policy Review, 13(3). doi:https://doi.org/10.14763/2024.3.1790.
15. Isagah, T. and Dhaou, B. (2024). Artificial intelligence readiness in Africa: Status quo and future research. Proceedings of the 2024 International Conference on AI Applications, pp.430–437. doi:https://doi.org/10.1145/3680127.3680199.
16. Jørgensen, B.N. and Ma, Z.G. (2025). Impact of EU regulations on AI adoption in smart city solutions: A review of regulatory barriers, technological challenges, and societal benefits. Information, 16(7), p.568. doi:https://doi.org/10.3390/info16070568.
17. Kaur, R., Gabrijelčič, D. and Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97(101804), pp.1–29. doi:https://doi.org/10.1016/j.inffus.2023.101804.
18. Khan, M.I., Arif, A., Khan, A.R.A., Anjum, N. and Arif, H. (2025). The dual role of artificial intelligence in cybersecurity: Enhancing defense and navigating challenges. International Journal of Innovative Research in Computer Science and Technology, 13(1), pp.62–67. doi:https://doi.org/10.55524/ijircst.2025.13.1.9.
19. Kharbanda, V., Seetharaman, A. and Maddulety, K. (2023). Application of artificial intelligence in cybersecurity. International Journal of Security and Privacy in Pervasive Computing, 15(1), pp.1–13. doi:https://doi.org/10.4018/ijsppc.318676.
20. Kumar, S. (2019). How AI & machine learning can help with government cyber security strategies. Xlpat. 30 July. Available at: https://en.xlpat.com/how-ai-machine-learning-can-helpwith-government-cyber-security-strategies/
21. Ledbetter, L. (2022). Defense Advanced Research Projects Agency (DARPA). Webopedia. Available at: https://www.webopedia.com/definitions/darpa/ [Accessed 26 Sep. 2025].
22. LG CNS (2016). Intelligence and security. LG CNS Blog. 7 November. Available at: https://blog.lgcns.com/1247
23. Mary, B.J. (2025). Artificial intelligence as an anti-corruption tool (AI-ACT): Potentials and pitfalls for top-down and bottom-up approaches. ResearchGate. Available at: https://www.researchgate.net/publication/391662548_Artificial_Intelligence_as_an_Anti-Corruption_Tool_AI-ACT_-Potentials_and_Pitfalls_for_Top-down_and_Bottom-up_Approaches.
24. Peredy, Z., Julaiti, K. and Laki, B. (2022). New opportunities of the Chinese companies in the big data era. Employment, Education and Entrepreneurship (EEE-2022) Conference Proceedings. Available at: https://www.researchgate.net/publication/364821564_New_Opportunities_of_the_Chinese_Companies_in_the_Big_Data_Era.
25. Perlman, A. (2019). The growing role of machine learning in cybersecurity. Security Roundtable. 18 June. Available at: https://www.securityroundtable.org/the-growing-role-ofmachine-learning-in-cybersecurity/
26. Perwej, Y., Abbas, S.Q., Dixit, J.P., Akhtar, N. and Jaiswal, A.K. (2021). A systematic literature review on the cyber security. International Journal of Scientific Research and Management, 9(12), pp.669–710. doi:https://doi.org/10.18535/ijsrm/v9i12.ec04.
27. Pina, E., Ramos, J., Jorge, H., Váz, P., Silva, J., Wanzeller, C., Abbasi, M. and Martins, P. (2024). Data privacy and ethical considerations in database management. Journal of Cybersecurity and Privacy, 4(3), pp.494–517. doi:https://doi.org/10.3390/jcp4030024.

28. Polyakov, M., Khanin, I., Shevchenko, G., Bilozubenko, V. and Korneyev, M. (2024). Systemic features of innovation development in the USA. Fìnansovo-kreditna dìâlʹnìstʹ: problemi teorìï ta praktiki, 1(54), pp.348–363. doi:https://doi.org/10.55643/fcaptp.1.54.2024.4247.
29. Raji, I. and Sholademi, D. (2024). Predictive policing: The role of AI in crime prevention. International Journal of Computer Applications Technology and Research, 13(10). doi:https://doi.org/10.7753/ijcatr1310.1006.
30. Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V. and Floridi, L. (2019). The Chinese approach to artificial intelligence: An analysis of policy and regulation. SSRN Electronic Journal. doi:https://doi.org/10.2139/ssrn.3469783.
31. Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V. and Floridi, L. (2020). The Chinese approach to artificial intelligence: An analysis of policy, ethics, and regulation. AI & Society, 36. doi:https://doi.org/10.1007/s00146-020-00992-2.
32. Skare, M. and Soriano, D.R. (2021). How globalization is changing digital technology adoption: An international perspective. Journal of Innovation & Knowledge, 6(4), pp.222–233. Available at: https://www.sciencedirect.com/science/article/pii/S2444569X21000202.
33. Themann, S. (2025). Challenges and strategies used in implementing AI governance: A systematic literature review. Available at: https://su.diva-portal.org/smash/get/diva2:1983756/FULLTEXT01.pdf [Accessed 12 Sep. 2025].
34. U.S. Department of War (2025). DARPA aims to develop AI, autonomy applications warfighters can trust. Available at: https://www.war.gov/News/News-Stories/Article/Article/3722849/darpa-aims-to-develop-ai-autonomy-applications-warfighters-can-trust/ [Accessed 26 Sep. 2025].
35. White & Case (2024). AI Watch: Global regulatory tracker – United States. White & Case LLP. Available at: https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states.
36. Wong, W., Wong, N.W.-M. and Hinnant, C. (2024). Adoption without transformation: AI and digital transformation in China and Taiwan. Proceedings of the 25th Annual International Conference on Digital Government Research, pp.807–814. doi:https://doi.org/10.1145/3657054.3657147.
37. Yazici, T. (2025). Toward a global standard for ethical AI regulation: Addressing gaps in AI-driven biometric and high-resolution satellite imaging in the EU AI Act. Law, Innovation and Technology, pp.1–29. doi:https://doi.org/10.1080/17579961.2025.2470589.
38. Yoo, G. (2017). Correlation between machine learning and information security. SK infosec Blog. 20 February. Available at: http://blog.naver.com/PostView.nhn?blogId=skinfosec2000&logNo=220937047579
39. Zou, M. and Zhang, L. (2025). Navigating China’s regulatory approach to generative artificial intelligence and large language models. Cambridge Forum on AI: Law and Governance, 1. doi:https://doi.org/10.1017/cfl.2024.4.