Balancing Innovation and Compliance: The Impact of the EU AI Act on AI-driven Cybersecurity Solutions in Healthcare

Ilkka Tikanmäki[1 2] and Jyri Rajamäki[1]

[1]Business, Data Processing and Service Sector Unit, Laurea University of Applied Sciences, Espoo, Finland

[2]Department of Warfare, National Defence University, Helsinki, Finland

Ilkka.tikanmaki@laurea.fi
jyri.rajamaki@laurea.fi

Abstract: The focus of the study is on the impact of the EU AI Act on AI-based cybersecurity solutions in healthcare. Adopting AI in healthcare cybersecurity is expected to enhance threat identification, bolster operational stability, and safeguard against increasingly complex cyber threats. The European Union's AI Act mandates new regulatory requirements for AI systems utilised in high-risk settings, particularly in healthcare. This study investigates the EU AI Act's influence on the creation and implementation of AI-driven cybersecurity solutions, focusing on representative AI-based cybersecurity solutions used in healthcare environments. Qualitative research methods were employed via a literature review and policy analysis of the EU AI Act, healthcare cybersecurity regulations, and global AI governance systems. The research contrasts the EU's AI regulation with the NIST AI risk management framework and the OECD AI principles and evaluates how AI-enabled cybersecurity functions align with key regulatory criteria such as risk assessment, disclosure, human supervision, and system stability. The findings indicate that AI-driven cybersecurity tools can assist in regulatory adherence and enhance healthcare stability, contingent upon organisations establishing robust governance frameworks, detailed practices, and human supervision mechanisms. Additional actions are required to achieve full alignment with the new transparency and accountability mandates, though existing systems demonstrate robust support for operational security and decision-making. The investigation finds that the EU AI regulation should be considered not just as a requirement to comply with but also as a chance to enhance the reliability, transparency, and enduring viability of AI-driven healthcare security systems.

Keywords: Artificial intelligence, EU AI Act, Healthcare cybersecurity, AI regulation, Human oversight

1. Introduction

Artificial Intelligence regulation is becoming important globally, especially in the European Union (EU). As regulations affect people's daily lives, they are interested in understanding the implications of regulations to understand the ethical and safe use of AI. AI and machine learning has shown a promising shift towards more efficient, accurate, and accelerated recovery processes, contributing to improved data protection strategies and operational efficiency (Bertrand & Leone, 2023). The AI law, which was introduced in April 2021, is focused on creating a standardised legal framework for the creation, marketing, and use of vetted AI systems in the EU (European Parliament, 2025). The law utilises a risk-based methodology to categorise AI systems into four risk levels: unacceptable, high, limited, and low or minimal risk.

AI systems, considered a direct danger to human safety, livelihoods, and rights, are considered an unacceptable risk. AI use cases that may pose significant threats to health, safety, or fundamental rights are categorised as high-risk use cases. The concept of limited risk is centred around the requirement for transparency in the use of AI; users should know they are dealing with a machine. AI rules that are considered minimal or risk-free are not included in the AI Act. This category is where most AI systems currently in use in the EU fall into. Examples of this include AI-powered video games or spam filters (European Commission, 2025).

The law forbids harmful AI practices, regulates high-risk AI systems, enforces transparency requirements on limited-risk systems, and grants low- or minimal-risk systems the freedom to operate without any additional obligations. (Madiega, 2023). The EU AI law has two main dimensions: 1. Regulatory content: The law requires compliance assessment of high-risk AI systems, promotes innovation with a regulatory testing environment, and defines enforcement authorities and penalties (European Parliament, 2025; Matheson LLP, 2024). 2. Stakeholder views: Some stakeholders support a narrower definition of AI to prevent overregulation. Civil rights organisations are calling for stricter rules, especially regarding biometric applications and proactive policing (Madiega, 2023). The Council and the Parliament of the European Union are actively involved in the legislative process of the AI law. The focus of the discussions is on key themes such as definitions, prohibited practices, high-risk AI systems, governance, enforcement and research and innovation. The Parliament's negotiating position includes significant changes to the Commission's original proposal (Council of the European Union, 2023).

The goal of the amendments is to connect the definition of AI systems with the Organisation for Economic Co-operation and Development (OECD) definition (OECD, 2024a). The other objectives include expanding the list of prohibited practices, clarifying the classification of high-risk AI systems, regulating general-purpose AI and foundation models, strengthening governance and enforcement mechanisms, and supporting research and innovation (Madiega, 2023).

The study aims to examine how emerging EU AI regulations influence the governance, development, and deployment of AI-enabled cybersecurity solutions in healthcare environments. The research question is 'How do EU AI regulations influence the governance, development, and deployment of AI-driven cybersecurity solutions in healthcare?'

The structure of this article is as follows: Section 2 examines the literature and gives in on current research. The methodology and data used in the study are presented in Section 3. Section 4 outlines the research findings and identified shortcomings, Section 5 concludes the study by summarising the key findings, discussing their implications, and suggesting future research directions.

2. Related Work

2.1 Trustworthy AI and AI Governance

The increasing adoption of artificial intelligence across critical sectors has highlighted the need for governance frameworks that ensure AI systems remain trustworthy, accountable, and aligned with societal values. In the European context, the concept of Trustworthy AI has emerged as a key foundation for AI governance. Trustworthy AI is generally understood as AI that is lawful, ethical, and technically robust throughout its lifecycle. Existing governance frameworks emphasize requirements such as human oversight, transparency, accountability, privacy and data governance, technical robustness, and fairness. These principles seek to ensure that AI systems support human decision-making while minimizing risks to individuals and society (ALTAI project, 2020).

AI governance can be viewed as the set of organizational structures, processes, and practices through which AI systems are designed, deployed, monitored, and controlled. Rather than focusing solely on algorithmic performance, contemporary governance approaches emphasize lifecycle management, documentation, accountability mechanisms, and continuous oversight. Such governance capabilities are particularly important in high-risk domains where AI-generated outputs may influence safety-critical decisions or affect fundamental rights (Rajamäki & Savolainen, 2026).

Several governance frameworks have been developed to support trustworthy and responsible AI. The OECD AI Principles (OECD, 2024a, 2024b) provide high-level guidance based on human-centred values, transparency, robustness, and accountability. Similarly, the NIST AI Risk Management Framework (National Institute of Standards and Technology, 2021) promotes a lifecycle-oriented approach to identifying, measuring, managing, and governing AI-related risks. While these frameworks are largely voluntary, they have significantly influenced international AI governance discourse and regulatory developments.

2.2 The EU AI Act and High-risk AI Systems

The European Union Artificial Intelligence Act represents the first comprehensive regulatory framework specifically addressing artificial intelligence. The regulation adopts a risk-based approach that classifies AI systems into unacceptable-risk, high-risk, limited-risk, and minimal-risk categories. The most stringent requirements apply to high-risk systems, where potential impacts on health, safety, critical infrastructure, or fundamental rights are considered significant.

The AI Act introduces obligations related to risk management, transparency, human oversight, technical robustness, accuracy, cybersecurity, and record keeping. Organizations deploying high-risk AI systems must establish processes for identifying and mitigating risks throughout the system lifecycle and maintain appropriate documentation demonstrating regulatory compliance. In contrast to governance frameworks such as NIST AI RMF and OECD AI Principles, the AI Act introduces legally binding requirements and formal enforcement mechanisms.

Despite its ambitious goals, several challenges have been identified in the literature. Researchers have noted uncertainties regarding enforcement mechanisms, transparency obligations, and the role of conformity assessment bodies. In addition, concerns have been raised that static regulatory structures may struggle to keep pace with the rapidly evolving capabilities of AI systems and emerging use cases. These concerns highlight the

importance of complementing regulatory compliance with continuous governance and risk-management practices.

The following Table 1 examines the disadvantages and uncertainties of the EU AI law.

Table 1: Disadvantages and uncertainty. Adapted from (Veale & Zuiderveen Borgesius, 2021)

Disadvantage	Uncertainty
Outdated Regulatory Framework	Uncertain Role of "Notified Bodies"
Potential for Limited National Regulations	Challenges with Transparency Obligations
Weak Enforcement Mechanisms	Limited User Participation in Enforcement

The law relies on outdated regulatory frameworks that may not be well-suited to the complexity and rapid development of AI. The specific risks posed by AI systems may not be addressed by these regulations (European Commission, 2025; Oladokun, 2025). The role of notified bodies is uncertain. The law requires notified bodies to evaluate high-risk AI systems. It is unclear how these bodies are selected and monitored. The necessary AI expertise may be lacking to assess these systems effectively. Moreover, the law allows service providers to assess their systems independently in numerous instances, which can lead to loopholes (Veale & Zuiderveen Borgesius, 2021).

Transparency obligations are not easy to enforce due to unclear transparency requirements for manipulated media and synthetic content. Identifying deepfake content and holding service providers accountable for misleading content may be difficult for users (Romero Moreno, 2024). Although a public database of high-risk systems may be beneficial for public oversight, it doesn't give users the ability to directly report problems or hold service providers accountable. User participation in the enforcement of the law is limited by this. (Veale & Zuiderveen Borgesius, 2021). Any reviews or research on how the new regulations apply to cyber threat intelligence sharing are slim, which highlights the unexploredness nature of this topic.

2.3 Artificial Intelligence in Cybersecurity and Cyber Threat Intelligence

Artificial intelligence has become an increasingly important component of modern cybersecurity operations. AI techniques are widely used for anomaly detection, threat intelligence analysis, intrusion detection, malware classification, automated incident response, and security operations centre (SOC) support. By processing large volumes of data and identifying patterns that may be difficult for human analysts to detect, AI can improve situational awareness and accelerate defensive decision-making (Bertrand & Leone, 2023; Oladokun, 2025).

Research has shown that AI-enabled cybersecurity solutions are particularly valuable in cyber threat intelligence (CTI) environments. AI can support the collection, correlation, analysis, and prioritization of threat information from heterogeneous sources, helping organizations understand evolving threat landscapes and respond more rapidly to cyber incidents. Machine-learning methods have demonstrated potential for improving the accuracy and efficiency of threat detection processes while reducing analyst workload (Bertrand & Leone, 2023).

Previous studies have also highlighted the strategic role of AI in critical infrastructure protection. In the energy sector, AI-supported CTI platforms have been shown to improve threat analysis, support decision-making processes, and strengthen cyber resilience by enabling more proactive security operations (Rajamäki et al., 2025). However, these benefits are accompanied by governance challenges related to trustworthiness, explainability, accountability, and the quality of underlying threat intelligence data.

2.4 AI-enabled Cybersecurity in Healthcare

Healthcare environments present a particularly demanding context for AI-enabled cybersecurity. Digital healthcare ecosystems increasingly rely on interconnected medical devices, cloud services, electronic health records, and external data-sharing mechanisms, creating a large and complex attack surface. Cyber incidents can directly affect patient safety, service continuity, operational resilience, and public trust. Consequently, cybersecurity measures implemented in healthcare settings must satisfy both technical and regulatory requirements.

Recent studies emphasize the value of AI-based approaches in detecting abnormal behaviour, identifying cyber threats, supporting ransomware defence, and improving incident response capabilities in healthcare environments. Adaptive and self-learning technologies have been identified as particularly useful in addressing the evolving threat landscape associated with Internet of Medical Things (IoMT) devices and increasingly sophisticated cyberattacks (Oladokun, 2025).

At the same time, healthcare cybersecurity raises important governance concerns. Decisions supported by AI systems may influence security actions affecting clinical operations and patient services, making human oversight essential. Transparency, explainability, accountability, privacy protection, and technical robustness therefore become key requirements for trustworthy deployment. These governance requirements closely align with the principles promoted by Trustworthy AI frameworks and the obligations established by the EU AI Act (Rajamäki & Savolainen, 2026).

2.5 Research gap

While substantial research exists on AI governance frameworks, AI-based cybersecurity, and healthcare cybersecurity separately, relatively limited attention has been paid to the intersection of these domains. Existing studies have examined trustworthy AI principles, regulatory frameworks, and AI-supported cyber threat intelligence, but fewer studies have investigated how emerging AI governance requirements affect the design, deployment, and operation of AI-enabled cybersecurity solutions within healthcare environments.

This gap is particularly relevant following the adoption of the EU AI Act, which introduces new compliance obligations for organizations deploying AI systems in potentially high-risk healthcare contexts. Consequently, understanding how regulatory requirements related to risk management, transparency, accountability, human oversight, and technical robustness influence healthcare cybersecurity solutions remains an important area for further investigation.

3. Method

The study examines the primary elements of EU AI requirements and how they affect the development and deployment of AI-enabled security platforms in healthcare ecosystem through a literature review and analysis of policy documents. A literature review was conducted from February to June 2026, using databases such as EBSCOhost, Google Scholar, and ScienceDirect. Search terms included variations like "EU AI Act," "artificial intelligence regulation," "AI governance," "healthcare cybersecurity," "cyber threat intelligence," and "trustworthy AI." It is essential that the scientific source material for this study also includes research related to the AI law itself, examining its key content. To obtain previously researched information on the topic, a literature review was conducted using modern sources. The evaluation reviewed peer-reviewed scientific journals, conference papers, EU official documents, and globally recognized standards published from 2021 to 2025. Online sources and relevant literature were used in the primary research format to ensure a comprehensive understanding of the topic. The state-of-the-art, challenges, and gaps in the field can be gained by conducting a comprehensive review of the existing literature.

Key EU directives are identified and evaluated by the study through a literature review and analysis of policy documents, which assess their impact on the development and deployment of AI technologies in platform ecosystems. Through practical insights, the results offer practical ways for platforms to navigate the complexity of regulation while promoting responsible use of AI. Secondary research methods are employed due to the complexity of the topic. This means that data collected by other researchers and experts is synthesised and analysed. Content analysis is one of the qualitative methods used in the research. Existing and verified documents, publications, and articles are the source of data analysis.

As the maturity of AI systems has recently been rising quickly, the research field is still quite young. There is some existing research done on applying AI to cyber threat intelligence gathering and analysis (Zhang et al., 2022). The research material consists of official EU AI Act documents and regulatory updates, complemented by scientific literature on AI governance, AI-assisted cyber threat intelligence (CTI) collection, and related cybersecurity use cases. Sources related to AI governance, regulatory compliance, healthcare cybersecurity, AI-driven cyber threat intelligence, and the EU AI Act were included. Selected publications describing healthcare cybersecurity platforms and AI-powered threat detection systems were also used as source material. The exclusion criteria included duplicate publications, non-English sources, studies unrelated to healthcare or cybersecurity, and those not addressing regulatory or high-risk contexts in specialised AI fields. Exclusion criteria included also non-European regulatory frameworks and sources that solely focused on general-purpose AI with no relevance to high-risk or healthcare contexts.

4. Results

This research investigated the influence of EU AI regulations on the architecture, implementation, and management of AI-driven cybersecurity methods within healthcare settings (Costa & Mendonça, 2025). To enhance understanding of trustworthy and responsible AI, the study covers compliance requirements

concerning transparency, risk management, reliability, and human oversight (Jenko et al., 2025). Additionally, the study provided practical perspectives by examining and illustrating how AI-based cybersecurity strategies can strike a balance between innovation and regulatory compliance in critical infrastructure sectors. Timely findings contribute significantly to both researchers and practitioners working on trustworthy AI systems, as governance and regulation of AI continue to grow in importance.

4.1 Assessment Outcomes

The table below presents comparisons of the EU AI Act (European Parliament, 2025), NIST AI RMF (National Institute of Standards and Technology, 2021) and the OECD AI Principles (OECD, 2024b).

Table 2: Comparison of the EU AI Act and International Frameworks

Framework	Nature	Approach	Focus Area	Applicability	Strengths
EU AI Act	Legally binding regulation	Risk-based classification (Unacceptable, High, Limited, Minimal)	Transparency, auditability, human oversight, enforcement	Mandatory for AI systems in the EU, especially high-risk sectors	Strong legal enforcement, clear obligations, public oversight
NIST AI RMF	Voluntary guidance	Lifecycle-based risk management (Govern, Map, Measure, Manage)	Trustworthiness, fairness, explainability, resilience	Flexible use by developers, deployers, and users of AI systems	Promotes internal governance and continuous improvement
OECD AI Principles	International policy guidelines	High-level ethical principles	Human-centred values, robustness, accountability, inclusive growth	Adopted by 46 countries; basis for national strategies	Encourages global alignment and ethical AI development

Table 3: Illustrative alignment of AI-enabled healthcare cybersecurity functions with selected EU AI Act requirements

EU AI Act Requirement	Regulatory Expectation	AI-enabled cybersecurity solutions	Indicative alignment based on the reviewed literature
Article 9 Risk Management	Continuous identification and mitigation of risks	AI-based anomaly detection and threat monitoring in healthcare networks	Partial alignment
Article 13 Transparency	Users must understand system outputs and limitations	Security alerts and mitigation recommendations are provided to operators	Partial alignment
Article 14 Human Oversight	Human intervention must remain possible	Information Security Manager receives alerts and makes final decisions	Strong conceptual alignment
Article 15 Accuracy & Robustness	Reliable, resilient and secure operation	Real-time monitoring and threat detection support cybersecurity resilience	Moderate to strong conceptual alignment

Operational decision-making continues to be handled by security professionals, with human oversight being particularly well supported. Transparency is partially addressed through alerts and suggestions, yet additional mechanisms for explainability may be needed to comply with future regulatory requirements (Kotte, 2024). Similarly, risk management and operational reliability functions are included via anomaly detection and ongoing monitoring mechanisms, though formal compliance procedures and documentation practices must be enhanced significantly to achieve full adherence to regulations.

AI-enabled cybersecurity solutions increasingly integrate cyber threat intelligence functions such as threat correlation, anomaly detection, and contextual threat analysis. These capabilities support the risk management and situational awareness requirements emphasized by the EU AI Act.

Beyond technical performance, the EU AI Act places increasing emphasis on accountability. Healthcare organisations deploying AI-enabled cybersecurity systems must be able to document decision processes, maintain audit trails, and demonstrate compliance throughout the system lifecycle. As well, the requirements

of the EU AI Act extend across the entire AI lifecycle, including design, deployment, operation, monitoring, and continuous improvement.

4.2 Governance Implications for Healthcare Cybersecurity

The increasing integration of artificial intelligence into healthcare cybersecurity presents significant governance challenges that extend beyond purely technical considerations. While AI-enhanced cybersecurity solutions can improve threat detection, incident response, vulnerability management, and cyber threat intelligence processing, they also introduce new requirements related to transparency, accountability, regulatory compliance, and human oversight. Consequently, healthcare organizations must ensure that cybersecurity governance frameworks evolve alongside emerging AI capabilities.

One of the most important governance implications concerns the need for trustworthy and explainable decision-making. Healthcare organizations operate in highly regulated environments where cybersecurity decisions may directly affect patient safety, service availability, and the protection of sensitive health data. AI-assisted cybersecurity tools, therefore, require sufficient transparency to allow security personnel and organizational leadership to understand, validate, and challenge automated recommendations. This is particularly important when AI is used to prioritize incidents, identify anomalies, or support threat intelligence analysis. Excessive reliance on opaque or poorly understood systems may increase operational risk and weaken organizational accountability.

A second implication relates to human oversight and responsibility allocation. Although AI can significantly enhance cybersecurity operations, responsibility for security decisions ultimately remains with human actors. Effective governance structures should therefore clearly define roles, decision rights, escalation procedures, and accountability mechanisms for AI-supported cybersecurity activities. Such arrangements help prevent overreliance on automated recommendations while ensuring that cybersecurity professionals remain capable of exercising professional judgment during complex or novel incidents.

Data governance represents another critical consideration. Healthcare cybersecurity increasingly depends on large volumes of operational, clinical, and threat intelligence data. At the same time, healthcare organizations must comply with stringent privacy and data protection requirements, including the General Data Protection Regulation (GDPR), the European Health Data Space (EHDS), and emerging AI-related regulatory frameworks. Governance mechanisms should therefore address data quality, access control, traceability, retention policies, and lawful information sharing. Maintaining public trust requires demonstrating that cybersecurity measures protect both organizational assets and patient privacy.

The findings further suggest that AI governance should be integrated into broader organizational risk management and cybersecurity governance processes rather than treated as an isolated technology initiative. Existing governance frameworks often focus on technical controls and regulatory compliance, whereas AI-enabled systems require continuous monitoring of algorithmic performance, model drift, bias, explainability, and emerging risks. Integrating AI governance into existing cybersecurity management structures enables organizations to establish consistent risk assessment practices and ensure alignment with strategic objectives.

From a cyber threat intelligence perspective, governance plays a central role in supporting information sharing and collaborative resilience. Healthcare organizations increasingly participate in national and international cybersecurity ecosystems where threat intelligence, vulnerability information, and situational awareness are exchanged among trusted stakeholders. Effective governance arrangements can facilitate such collaboration by establishing common standards for information quality, confidentiality, trust, and accountability. AI technologies may further enhance these collaborative processes by supporting threat prioritization, pattern recognition, and early warning capabilities, provided that appropriate safeguards are implemented.

The assessment approach proposed in this study demonstrates how governance-oriented evaluation mechanisms can support responsible adoption of AI within healthcare cybersecurity environments. By aligning cybersecurity assessment activities with established trustworthy AI principles, organizations can better balance operational efficiency, regulatory compliance, ethical considerations, and stakeholder trust. Rather than viewing AI governance solely as a compliance requirement, healthcare organizations may benefit from treating it as a strategic capability that strengthens cyber resilience, supports informed decision-making, and enhances preparedness for evolving cyber threats.

Overall, the results indicate that future healthcare cybersecurity strategies should combine technical safeguards with governance mechanisms that promote transparency, accountability, human oversight, and continuous

improvement. Such an approach is increasingly necessary as AI becomes more deeply embedded in cybersecurity operations and decision-support processes across the healthcare sector.

5. Discussion and Conclusions

The study examined how new EU AI regulations affect the design, management and deployment of AI-based cybersecurity solutions in healthcare. The findings indicate that EU AI regulations place substantial compliance demands on healthcare AI applications. Depending on their intended purpose and operational context, some AI-enabled cybersecurity systems used in healthcare may fall within, support or interact with high-risk AI use contexts.

Adherence to EU AI regulations extends beyond technical excellence and necessitates the establishment of robust governance frameworks, risk assessment protocols, disclosure mechanisms, and human oversight mechanisms by organisations. A comparison between the NIST AI Risk Management Framework and the OECD AI Principles underscores that both aim to promote trustworthy and accountable AI systems. The EU AI regulation imposes enforceable standards that entities must comply with throughout an AI product's lifecycle.

The illustrative assessment demonstrates that AI-driven security features, including threat identification, anomaly monitoring, and decision assistance, can facilitate regulatory adherence and enhance resistance against changing cyber threats. Additionally, the findings show that obtaining compliance will necessitate additional efforts in explainability, documentation, auditing, and continuous compliance assessments. In healthcare settings, it became clear that human oversight was a crucial requirement, with AI meant to augment professional decision-making rather than take over.

In practice, the findings emphasise that regulatory adherence and technological advancement should not be viewed as conflicting objectives. Alternatively, EU AI guidelines can provide a foundation for creating trustworthy, transparent, and accountable AI solutions that bolster cybersecurity and enhance public confidence in digital healthcare services. Groups that actively incorporate regulatory stipulations into their system development are probably going to gain lasting advantages in areas like resilience, credibility, and operational steadiness.

The findings suggest that compliance with the EU AI Act should not be understood solely as a regulatory obligation. Instead, AI governance can be viewed as an organisational capability comprising risk management, transparency, accountability, documentation practices, and human oversight mechanisms. Healthcare organisations that embed these capabilities into their cybersecurity operations are likely to be better prepared for both regulatory scrutiny and evolving cyber threats.

For future research, examining AI-based cybersecurity techniques through empirical case studies and the actual application of resilience within healthcare facilities could be explored. Further studies might investigate how EU AI compliance aligns with other regulatory bodies like NIS2, GDPR, and the Cybersecurity Act. A deeper investigation could examine how these merged requirements influence the deployment of AI-driven cyber threat intelligence and security operations platforms.

Acknowledgements

This study has received funding from the Cybersecurity in Everyday Work in the Social and Healthcare Sector (KyberSoTe) project. The views expressed are those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Ethics Declaration: Ethical clearance was not required for the research.

AI Declaration: The paper's spelling was verified using the artificial intelligence tool.

References

ALTAI project. (2020). *The Assessment List for Trustworthy Artificial Intelligence*. Home Page - ALTAI. https://altai.insight-centre.org/

Bertrand, C., & Leone, M. (2023). *How AI might change the data protection space*. Tech Target. https://www.techtarget.com/searchdatabackup/opinion/How-AI-might-change-the-data-protection-space

Costa, H., & Mendonça, J. (2025). Assessing European Union Member States' Implementation of the Artificial Intelligence Act. In R. Zimmermann, J. C. Rodrigues, A. Simoes, & G. Dalmarco (Eds.), *Human-Centred Technology Management for a Sustainable Future* (pp. 243–253). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-72494-7_24

Council of the European Union. (2023, September 12). *Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world* [Press Release]. Consilium. https://www.consilium.europa.eu/en/press/press-

releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/

European Commission. (2025, August 1). *AI Act: Shaping Europe's digital future*. AI Act. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

European Parliament. (2025, February 19). *EU AI Act: First regulation on artificial intelligence*. European Parliament Directorate General for Communication. https://www.europarl.europa.eu/pdfs/news/expert/2023/6/story/20230601STO93804/20230601STO93804_en.pdf

Jenko, S., Papadopoulou, E., Kumar, V., Overman, S. S., Krepelkova, K., Wilson, J., Dunbar, E. L., Spice, C., & Exarchos, T. (2025). Artificial Intelligence in Healthcare: How to Develop and Implement Safe, Ethical and Trustworthy AI Systems. *AI*, *6*(6), 116. https://doi.org/10.3390/ai6060116

Kotte, G. (2024). AI-Powered Automated Incident Response in Healthcare Cybersecurity Operations. *International Journal of All Research Education and Scientific Methods*, *12*(10), 3369–3375. https://doi.org/https://doi.org/10.56025/ijaresm.2025.1210243369

Madiega, T. A. (2023). *General-purpose artificial intelligence*. European Union. https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2023)745708

Matheson LLP. (2024). *The EU Artificial Intelligence Act: A Guide for Businesses*. Matheson. https://www.matheson.com/docs/default-source/content-library/matheson-ai-act-guide.pdf?sfvrsn=87d56e14_3

National Institute of Standards and Technology. (2021, July 12). *AI Risk Management Framework* [Framework]. NIST. https://www.nist.gov/itl/ai-risk-management-framework

OECD. (2024a). *Explanatory memorandum on the updated OECD definition of an AI system* (OECD Artificial Intelligence Papers DSTI/CDEP/AIGO(2023)8/FINAL; OECD Artificial Intelligence Papers, p. 11). Organisation for Economic Co-Operation and Development (OECD). https://doi.org/10.1787/623da898-en

OECD. (2024b). *OECD Legal Instruments* (Recommendation OECD/LEGAL/0449; p. 25). OECD. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Oladokun, P. (2025). Mitigating Cybersecurity Risks in Healthcare with AI: Developing Adaptive Defense Models Against Emerging Threats. *IJFMR - International Journal For Multidisciplinary Research*, *7*(3), 1–18. https://doi.org/10.36948/ijfmr.2025.v07i03.46651

Rajamäki, J., & Savolainen, K. (2026). *From Trustworthy AI to Superintelligence Governance: Lessons from the ALTAI Framework and SHAPES Pilots* (No. 2026080643). Preprints. https://doi.org/10.20944/preprints202608.0643.v1

Rajamäki, J., Tikanmäki, I., Knowlton, R., & Korhonen, S. (2025). AI and Cyber Threat Intelligence Management in the Energy Sector. *European Conference on Knowledge Management*, *26*(2), 1326–1330. https://doi.org/10.34190/eckm.26.2.3781

Romero Moreno, F. (2024). Generative AI and deepfakes: A human rights approach to tackling harmful content. *International Review of Law, Computers & Technology*, *38*(3), 297–326. https://doi.org/10.1080/13600869.2024.2324540

Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, *22*(4), 97–112.

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K.-K. R. (2022). Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *Artificial Intelligence Review*, *55*(2), 1029–1053. https://doi.org/10.1007/s10462-021-09976-0