DYNAMO and the EU AI Act: Balancing Innovation and Regulation

Ilkka Tikanmäki[1,2], Jyri Rajamäki[1,2], Elina Johnston[1], Jan Salenius[1], Jenna Teräväinen[1], Petri Tuovila[1], Peik Feiring[1], Maria Sissonen[1], André Winberg[1] and Krishia Ybañez[1]

[1]Security and Risk Management, Laurea University of Applied Sciences, Espoo, Finland
[2]National Defence University, Helsinki, Finland

Ilkka.tikanmaki@laurea.fi

Abstract: This work-in-progress paper examines the impact of the European Union's Artificial Intelligence Act (EU AI Act) on the EU-funded cybersecurity project DYNAMO, which integrates Business Continuity Management (BCM) and Cyber Threat Intelligence (CTI) to enhance the resilience of critical sectors such as healthcare, transportation, and energy. The research analyses the requirements and implications of the EU AI Act on the DYNAMO platform, aiming to provide key insights for policymakers, and industry professionals, and the main goal is to facilitate informed decision-making and promote the ethical development of artificial intelligence in the EU. To achieve this, the ALTAI tool (Assessment List for Trustworthy Artificial Intelligence) can be used to ensure compliance with ethical principles in the DYNAMO project. The study addresses the research question: How does the EU AI Act affect the development, deployment, and operational efficiency of AI-driven cybersecurity solutions in the DYNAMO project? Through a comprehensive literature review and secondary research, the paper examines the regulatory environment focusing on data governance, algorithmic transparency, accountability, and ethical considerations. Results indicate that while the EU AI Act imposes stringent requirements on high-risk AI systems, such as those used by DYNAMO, it also offers opportunities for responsible innovation. As highlighted by the study, continuous collaboration and dialogue among stakeholders are crucial to navigating the evolving regulatory landscape. The findings underscore the need for robust cybersecurity strategies to comply with regulatory standards and enhance the security and resilience of critical infrastructures.

Keywords: European Union, AI requirements, DYNAMO, Regulatory framework, Data recovery

1. Introduction

There is a need to understand the impact of the EU AI Act on AI-driven cybersecurity solutions. The regulation of AI is a balancing act between enabling rapid innovation and ensuring the security of AI systems. Strict regulation imposes overhead on any new company working in AI development or usage, and it is crucial to assess how these regulations affect projects like DYNAMO (DYNAMO project, 2024).

The objectives of this work-in-progress paper are to: (1) analyse the requirements and implications of the EU AI Act on the DYNAMO platform; (2) provide key insights for policymakers, industry professionals, and academics; (3) facilitate informed decision-making and promote ethical AI development within the EU; and (4) focus on regulatory compliance, innovation, risk management, and stakeholder impact. The applied research methodology is a secondary study (Bermingham, 2020; Tegan, 2023), with the research question: "How does the EU AI Act affect the development, deployment, and operational efficiency of AI-driven cybersecurity solutions in the DYNAMO project?"

2. Literature Review

AI plays a significant role in cybersecurity, for example, by enhancing the recovery process, prioritising essential systems based on their information dependencies, and reducing downtime. AI has revolutionised data recovery by advancing data protection strategies and operational efficiency. It smartly prioritises essential systems based on information dependencies, reducing recovery periods and downtime (Nivedhaa, 2024). The intelligent data retrieval approach takes advantage of machine learning models to refine the precision and velocity of the retrieval process, marking a significant advancement in data protection strategies and operational efficacy (Khaleel et al., 2024).

The EU has introduced the EU AI Act, aiming to establish a comprehensive legal framework governing the development and use of AI within its jurisdiction (European Union, 2024; Hoffman, 2009; Laux et al., 2024; Madiega, 2023). It necessitates AI systems being safe, transparent, traceable, non-discriminatory, and environmentally friendly and mandates human oversight. The EU AI Act adopts a risk-based approach, categorising AI systems into four levels of risk, with corresponding prohibitions, regulations, and transparency requirements. Controversial issues have emerged from stakeholder feedback, particularly concerning definitions and the risk-based methodology. The EU Parliament is working to refine the legislation, suggesting amendments to align with international standards, broaden the range of banned practices, and enhance governance and enforcement measures (Madiega, 2023). The ALTAI tool provides a comprehensive assessment list that helps

ensure AI systems adhere to ethical principles, enhancing the discussion on privacy, data ownership, consent, and transparency (European Commission, 2019).

The EU AI Act categorises AI systems into four risk levels: unacceptable risk, high risk, limited risk, and minimal risk. Unacceptable risk includes cognitive manipulation, social scoring, and biometric categorisation. High-risk systems, such as those managing critical infrastructure, must adhere to stringent regulations, including risk management, data governance, and human oversight. Given the Dynamo project's focus on securing critical infrastructure understanding these implications is crucial. A deployer is any entity using an AI system under its authority, except when used for personal non-professional activities. An entity or individual that implements and uses high-risk considered AI systems, is known as a "high-risk AI system deployer."

The EU AI Act generally provides broad guidelines and base-level procedures for developers and deployers of AI systems. For high-risk systems, the act specifies how users should be protected against biases and what data can be used for training AI models. Article 10 outlines data governance requirements for high-risk systems, emphasising the need to consider potential biases and implement safeguards. Article 11 mandates creating and maintaining technical documentation before market deployment, with lighter requirements for small and medium-sized enterprises (European Parliament, 2023).

The EU AI Act mandates deployers and developers of AI systems establish a risk management system to assess and control risks throughout the AI system's lifecycle. Developers should implement mechanisms for effective human oversight, ensuring compliance with the regulations. Additionally, the Act demands AI systems meet security and fault tolerance standards (Laux et al., 2024).

Studies highlighted several concerns with the EU AI Act, including potential gaps in adapting the legislation to the current regulatory framework, the expertise of 'notified bodies', and the enforcement challenges related to transparency and synthetic content. These studies emphasise the need for effective regulatory compliance and the potential impact on innovation. A public database of high-risk AI systems aids in surveillance. However, the absence of direct reporting tools weakens user accountability and involvement in regulatory actions. According to (Veale & Zuiderveen Borgesius, 2021) there are gaps in adapting the legislation to the current regulatory framework, particularly regarding the dynamic and complex nature of AI systems. Relying on notified bodies to assess high-risk AI systems raises questions about their expertise and oversight mechanisms, compromising the effectiveness of assessments. Moreover, the duty of transparency concerning 'deepfakes' and synthetic content presents enforcement challenges, facilitating the dissemination of deceptive information. Additionally, the act's preemptive impact on national regulations raises concerns, as it may impede the capacity of member states to tackle specific social issues associated with AI. Furthermore, the act's enforcement mechanisms highlight deficiencies in the complaint procedures and user involvement (Veale & Zuiderveen Borgesius, 2021).

3. Results

3.1 Regulatory Environment

The European Union's cybersecurity strategy aims to enhance cyber resilience against threats and protect communications and data, ensuring that all citizens and businesses may benefit. To achieve this, the EU invests in cybersecurity programs and innovations like Horizon Europe (HE), Digital Europe Programmes (DEP), and the Connecting Europe Facility (CEF).

This study is based on the current situation, where is not yet possible to concretely assess the consequences brought by the regulations. The EU's AI Act has just been implemented during this study, and there is not enough data available to concretely assess the topic. The implementation should be carried out by the Data Act, the success of which should again be evaluated at sufficient intervals. Based on this it is possible to re-evaluate the success of the Act and implement possible corrective measures quickly so that possible failures or disadvantages cannot grow too large.

3.2 Impact on DYNAMO

DYNAMO is a comprehensive cloud platform integrating business continuity management (BCM) and cyber threat intelligence (CTI) to enhance resilience assessment and reduce cyberattacks in critical sectors. The EU AI Act imposes several obligations on high-risk AI system deployers, such as DYNAMO. These include adhering to technical instructions, assigning human oversight, maintaining logs, and monitoring and reporting any suspected malfunctions, risks, or threats immediately. The AI Act could bring significant changes to the DYNAMO platform, potentially impacting its development, deployment, and operational procedures. The ALTAI tool can assist the

DYNAMO project in meeting these stringent requirements by providing practical guidelines and best practices for ethical AI development and deployment. Depending on the risk level of the AI systems used by DYNAMO, the platform may need to comply with various requirements and obligations.

The AI Act categorises AI systems based on a risk-based approach. While certain AI systems with unacceptable risks are prohibited, a wide range of high-risk AI systems are permitted but subject to specific requirements and obligations. Depending on the risk level associated with the AI systems implemented by DYNAMO, the platform may be required to adhere to specific requirements and obligations outlined in the AI Act. The AI Act establishes specific regulations for general-purpose AI (GPAI) models and imposes stricter requirements for GPAI models with high-impact capabilities. If DYNAMO utilises such models, it will be obligated to comply with these regulations. The European Union's AI Act could bring significant changes to the DYNAMO platform. Depending on the risk level of the AI systems used by DYNAMO, the platform may need to comply with various requirements and obligations. This could potentially impact the operational procedures and services offered by DYNAMO.

3.3 Intelligent Data Recovery Solutions

Incidents of data loss present considerable challenges to both organisations and individuals, highlighting the essential need for effective data recovery solutions. The advent of AI presents a chance to transform data recovery methods, enhancing their accuracy, efficiency, and versatility in multiple situations. In the context of this study, a detailed research initiative was also presented that focused on examining the efficiency, enhancement, and real-world uses of AI algorithms in data recovery. This focused on creating innovative AI algorithms and frameworks specifically for data recovery tasks, assessing AI data recovery methods through benchmark datasets and real-world applications, performing a comparative study of various AI techniques, and determining optimisation strategies for the implementation of AI-driven data recovery solutions. The research objectives delved into investigating the effectiveness of AI algorithms for data recovery across different scenarios. This provided crucial data for developing conceptual AI-based techniques to enhance the accuracy and efficiency of data recovery. It also explored the potential applications of AI in data recovery within real-world contexts, such as cybersecurity, digital forensics, and disaster recovery.

3.4 Opportunities and Challenges

According to the EU AI Act DYNAMO is classified as a high-risk AI system deployer ("user"). The Act imposes several obligations on high-risk AI system deployers under Article 26. These include adhering to the technical instructions provided by the AI's developers, assigning human oversight, maintaining logs, and monitoring and reporting any suspected malfunctions, risks, or threats to the provider immediately. Applying the EU AI Act to EU-funded cybersecurity projects like DYNAMO presents several challenges. The new EU AI Act imposes obligations on deployers nearly as stringent as those for providers. Additionally, the obligations are broad and may lack clarity, making it difficult for stakeholders to interpret and understand the requirements and obligations.

Another challenge is potential liability. According to the EU AI Act, deployers must adhere to the provider’s technical and operational instructions. In case of malfunction, providers could argue that the deployer did not use the system according to these instructions. In other words, any potential liabilities may fall to deployers. Assigning human oversight when using AI systems is challenging because it requires thorough training, audits, and time. The EU AI Act mandates quality input data, which leads to a significant dependence on data. Ensuring quality input data is an ongoing issue. For instance, maintaining data integrity, standardisation, and preventing biases are challenges that may arise. The EU AI Act also requires AI system deployers to maintain a log every six months, which is demanding and challenging.

While the EU AI Act imposes stringent requirements, it also offers opportunities for responsible innovation. The results highlight the importance of continuous collaboration and dialogue among stakeholders to navigate the evolving regulatory landscape.

4. Discussion

The findings indicate that the EU AI Act imposes stringent requirements on high-risk AI systems, such as those used by DYNAMO, but also offers opportunities for responsible innovation. The study underscores the need for robust cybersecurity strategies to comply with regulatory standards and enhance the security and resilience of critical infrastructures.

DYNAMO aims to address the threats and risks posed by digitalisation in business organisations through business continuity management (BCM) and cyber threat intelligence (CTI). These organisations are crucial for the

functioning of critical infrastructures such as energy, health, and transport sectors. The implications for policymakers, industry professionals, and academics include the need for continuous collaboration and dialogue to navigate the evolving regulatory landscape. The study provides key insights to support informed decision-making and promote ethical AI development within the EU.

The balance between encouraging innovation and ensuring regulatory compliance is crucial. The ALTAI tool supports this balance by offering a structured approach to ethical AI, fostering continuous collaboration and dialogue among stakeholders to navigate the evolving regulatory landscape. The study explores how the EU AI Act impacts this balance and the potential for fostering responsible AI innovation while minimising risks. The EU AI Act aims to unify AI regulations throughout the EU by categorising AI systems according to their risk levels and imposing stricter rules on high-risk systems. By setting standards for AI systems used in cybersecurity, this regulation could impact cybersecurity research, as they must meet specific safety and transparency requirements. The DYNAMO project, which focuses on improving cybersecurity with innovative technologies, may require a re-alignment of its research and development activities with the AI Act requirements. This alignment has the potential to influence the development and implementation of new cybersecurity solutions, promoting innovation while ensuring compliance with regulatory standards. The future of cybersecurity research could be influenced by the interaction between the AI Act and the DYNAMO project, which balances innovation with regulatory compliance.

5. Conclusions

The EU AI Act aims to maintain responsible and transparent AI while using it effectively. The EU AI Act is new and follows a risk-based approach, setting broad requirements that may need further explanation and clarification. Communication gaps may also arise among authorities, business operators, AI system providers, and deployers due to different interpretations of the regulation. This study has examined the EU AI Act and its influence on the DYNAMO platform. It has investigated the convergence of these rules with aspects of data governance, algorithmic transparency, accountability, and ethical considerations. The EU's focus on responsible AI innovation highlights its dedication to promoting ethical standards and mitigating potential risks. Although compliance might pose challenges, it also provides opportunities for stakeholders to engage in responsible innovation.

It is crucial to maintain ongoing collaboration and dialogue between policymakers, industry experts, and researchers to successfully steer through the changing regulatory environment. The ALTAI tool plays a vital role in this process by providing concrete methods and practices to ensure responsible AI innovation and compliance with regulatory standards. Fostering a culture of responsible AI innovation is key to harnessing the advantages of AI while minimising potential risks to both individuals and the whole society. This study has the potential to offer significant insights to stakeholders, directing informed decision-making and influencing the evolution of AI technologies that comply with ethical standards and legal mandates within the DYNAMO framework and further afield. Recommendations for stakeholders include maintaining ongoing collaboration and dialogue, fostering a culture of responsible AI innovation, and ensuring compliance with regulatory standards to enhance the security and resilience of critical infrastructures.

Digitalization has offered endless opportunities and benefits but brings challenges and risks, including cyber threats. Authorities and organisations have committed funds and resources to cybersecurity innovations and research to combat these cybersecurity threats. AI is one of these innovations, and its use is widespread, both personally and professionally. Despite this, AI has weaknesses that should be researched. Future research should explore the impact of AI regulations on cybersecurity projects further focusing on the long-term effects of the EU AI Act and potential areas for improvement in regulatory compliance and innovation.

Acknowledgements

Acknowledgement is paid to the DYNAMO Project, funded by the European Union under grant agreement no. 101069601. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

References

Bermingham, R. (2020, September 8). Study designs: Secondary research [Resource]. UK Parliament. https://post.parliament.uk/study-designs-secondary-research/

DYNAMO project. (2024, January 9). DYNAMO Mission and Objectives. https://horizon-dynamo.eu/about/

European Commission. (2024, June 26). AI Act: Shaping Europe's digital future. AI Act. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

European Parliament. (2020, September 23). Artificial intelligence: Threats and opportunities. Topics | European Parliament. https://www.europarl.europa.eu/topics/en/article/20200918STO87404/artificial-intelligence-threats-and-opportunities

European Parliament. (2023, June 8). EU AI Act: First regulation on artificial intelligence. Topics | European Parliament. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

European Union. (2024, April 30). AI Act. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Hoffman, M. (2023, September 26). The EU AI Act: A Primer. Center for Security and Emerging Technology. https://cset.georgetown.edu/article/the-eu-ai-act-a-primer/

Khaleel, M., Jebrel, A., & Shwehdy, D. M. (2024). Artificial Intelligence in Computer Science: https://doi.org/10.5281/zenodo. 10937515. Int. J. Electr. Eng. and Sustain., 01-21.

Laux, J., Wachter, S., & Mittelstadt, B. (2024). Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk. Regulation & Governance, 18(1), 3–32. https://doi.org/10.1111/rego.12512

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

Nivedhaa, N. (2024). A Comprehensive Review of AI's Dependence on Data. International Journal of Artificial Intelligence and Data Science, 1(1), 1–11. https://doi.org/10.13140/RG.2.2.27033.63840

Tegan, G. (2023, January 20). What is Secondary Research? [Definition, Types, & Examples]. Scribbr. https://www.scribbr.com/methodology/secondary-research/

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