Navigating the Cyber Resilience Act: Implications for the Dynamo Horizon Project

Jyri Rajamäki, Petra Koskela, Sami Mehtonen, Verneri Lämsä, Sara Korpila and Tero Lämsä
Laurea University of Applied Sciences, Espoo, Finland

jyri.rajamaki@laurea.fi
petra.m.koskela@student.laurea.fi
sami.mehtonen@student.laurea.fi
verneri.lamsa@student.laurea.fi
sara.korpila@student.laurea.fi
tero.lamsa@student.laurea.fi

Abstract: This work-in-progress paper develops an operational model for the DYNAMO Horizon Europe Project to ensure compliance with the EU Cyber Resilience Act (CRA). Compliance with the CRA enables DYNAMO to provide a high level of security and maintain its competitiveness. By meeting the CRA requirements, DYNAMO can protect its users, strengthen its market position, and promote best practices in cybersecurity. The area in which DYNAMO works is critical to society, creating a complete platform of tools and frameworks for cyber threat intelligence. Tools included in the platform need to abide by the regulations in place and being compliant also helps DYNAMO ensure that the tools are safer for the users of its platform. The regulations cause complications and confusion without sufficient preparation. As a subject still under research, with pending regulation, this study provides future proofing and assistance in planning efficient transition to compliance. Compliance for third parties is simplified in regulation. Open-source software provides a powerful exception to this regulation as well, being useful as a method of risk transference through using these exceptions. DYNAMO can utilize these aspects of the CRA to enhance compliance. How different companies are fulfilling their vulnerability management regarding CRA is a venue for future research purposes, as are methods for futureproofing compliance, and the impacts of CRA on Artificial Intelligence use, and how this intersects with the AI Act.

Keywords: Cyber Resilience Act, Cyber resilience, DYNAMO project, Compliance, Open-source software, Design science

1. Introduction

The EU Cyber Resilience Act (CRA) aims to enhance cybersecurity across the EU's digital ecosystem, ensuring that digital products and services are secure throughout their lifecycle. The CRA creates a standardized legal framework to ensure that hardware and software products are designed, developed, and maintained with strong cybersecurity measures throughout their entire lifecycle. This regulation aims to reduce the risks associated with cyberattacks, which can significantly impact the economy, democracy, consumer safety, and health. The CRA requires manufacturers to comply with essential cybersecurity standards, perform risk assessments, and provide security updates, thereby promoting a safer digital environment across the EU (.

The DYNAMO Horizon Europe Project is a European Union initiative aimed at enhancing resilience against cyber threats. It focuses on creating a comprehensive platform of tools and frameworks for cyber threat intelligence. DYNAMO supports critical sector organizations in healthcare, energy, and transportation by providing tools for efficient threat detection, mitigation, and response (DYNAMO 2024).

This work-in-progress paper seeks to investigate the CRA and its requirements to analyze how it aligns with the DYNAMO project and the tools and services the project develops. As the main obligations of the act will apply from December 2027 onwards (European Commission 2024) it is crucial to incorporate them already during the development phase of the DYNAMO platform and tools. The paper's goal is to identify what changes, if any, are required for DYNAMO to become compliant with the CRA, and to propose actionable solutions for said obligations. As there is no existing research exploring the relationship between DYNAMO and the CRA, this paper aims to fill that gap. Furthermore, despite this study being aimed at DYNAMO, any company or organization manufacturing or retailing digital products within the EU can gain insights into some of the requirements and potential ways to become compliant.

2. Literature

The Cyber Resilience Act (CRA) is an EU-wide legislative proposal aimed at establishing mandatory cybersecurity requirements for products with digital elements throughout their entire lifecycle. The purpose of the Act is to harmonize cybersecurity rules within the EU and strengthen trust in digital and physical products (European Commission 2022). This Act directly affects products like DYNAMO tools, as they must meet the requirements set by the Act to be compliant in the market. (ENISA 2024, 3.) Additionally, research has found that while existing

standards like ISO 27001 exist, they do not fully cover all the requirements set by the CRA, and further standardization work is still needed (European Commission 2022). This highlights the need to develop and harmonize standards so that products like DYNAMO can comprehensively meet the requirements. (ENISA 2024, 59.)

Chiara (2022a) illuminates the 'horizontal' nature of the CRA proposal by emphasizing its key components. Specifically, his analysis considers the new obligations imposed on economic operators, the conformity assessment procedures, the market surveillance framework, and the interaction with other legislative initiatives, both within and outside the realm of EU cybersecurity law. Given the sector-specific regulatory approach previously adopted by the Commission for cybersecurity requirements, a horizontal intervention is necessary to ensure legal certainty, avoid redundant obligations, and prevent further market fragmentation (Chiara 2022).

IoT and other hyperconnected devices have made our daily lives easier and more convenient but also brought us a high risk of cyber threats at the same time. Attacks on these new hyperconnected devices are constantly evolving and becoming more advanced, impactful, and frequent. Chiara (2022b) highlights three main regulatory failures in IoT security: (1) Lack of mandatory requirements, (2) absence of a common legal basis for cybersecurity, and (3) no rules exist for post-market surveillance. The EU Cyber Resilience Act aims to address these ever-evolving challenges by safeguarding digital infrastructure and making our society more resilient to evolving cyber threats (Schmittner, et al. 2024). Regarding the cybersecurity challenges of IoT, the general broad wording of the CRA's requirements can lead to varying interpretations. This means that the effectiveness of the CRA in addressing the challenges of security during manufacturing, identification and authentication, large attack surfaces, and diverging standards and regulations largely depends on how harmonized standards develop and how the industry adopts them. (Shaffique 2024a).

The wording used in the Cyber Resilience Act might be somewhat vague and leave room for interpretations and legal uncertainty. The Cyber Resilience Act uses terms for example, “limit attack surfaces”, “appropriate level of cybersecurity” and “without any known exploitable vulnerabilities” but these are not properly defined in the Cyber Resilience Act and could allow for different levels of interpreting (Shaffique 2024a).

Noël (2024a) explains how the new CRA regulations alongside the U.S. Cyber Trust Mark set security principles but leave the how, optional. Within the scope of regulatory limitations are Data Protection, Cyber State Awareness, Vulnerability fixes, and Reduction of incidents’ impact. This leaves the Level of Security – the level of protection that must reflect the level of risk and Functional Requirements – for example, cryptographic algorithms, protocols, PKI solutions, and certificate formats outside of the scope. The Technological Implementations are thus left to the manufacturers of devices and producers of services like DYNAMO to figure out.

Burri and Zihlmann (2023) present the following criticisms of the EU's Cyber Resilience Act:

- Definitional Issues: There are ambiguities and gaps in the definitions within the CRA proposal, which could complicate its practical application.
- Coordination Problems: Harmonizing the CRA with existing and forthcoming EU legislation may be challenging, potentially leading to overlaps and conflicts.
- Fragmentation in Surveillance and Enforcement: Practices and resources of market surveillance authorities may vary across member states, leading to inconsistencies in enforcement.
- Challenges in Risk Classification: Most digital products are classified as low-risk, which could undermine overall cybersecurity. Additionally, the risk classification does not always consider the operational environment of the products.
- Role and Awareness of Users: The ability and willingness of users to respond to insecure products is uncertain, which could reduce the effectiveness of the CRA.
- Fragmentation of Global Data Governance: The CRA's potential role as a global cybersecurity standard-setter could lead to fragmentation in the global data governance framework and increase geopolitical tensions.
- Regulatory Adaptability: It is unclear whether the CRA can adapt to the rapidly evolving threat landscape, especially with emerging technologies like artificial intelligence.

Fedienko (2024) describes the European Central Bank's (ECB) cyber resilience efforts, highlighting the planned stress tests for 2024, which aim to assess how well banks can respond to and recover from cyber-attacks. These tests will involve 109 banks under ECB supervision, with 28 banks undergoing an extended assessment to provide additional information on their handling of cyber-attacks. This sample includes various business models and

geographic regions to ensure a comprehensive representation of the Eurozone banking system. The data obtained will be used for publication and further supervisory evaluation throughout 2024. The ECB's approach focuses on improving banks' capabilities to manage cyber threats and ensure operational continuity post-attack, rather than solely on preventing attacks. This strategy aims to enhance banks' preparedness and resilience in the face of evolving cyber threats (Fedienko 2024).

3. Methodology

The design science research (DSR) approach (Hevner et al. 2004), as shown in Figure 1, guides this work-in-progress paper, which aims to produce an operational guide for the DYNAMO project on how its developed DYNAMO platform and tools meet the requirements of the CRA. The relevance cycle of DSR connects the research to the DYNAMO project, and the rigor cycle to the knowledge base.

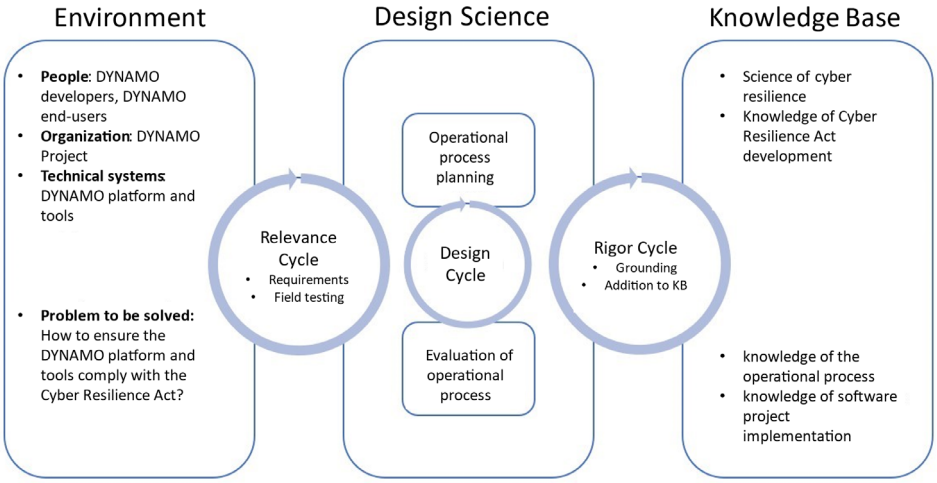

Figure 1: Design science framework of the paper (modified from Hevner el al. 2004)

This paper is working within the confines of fundamental conceptual research as defined in the Handbook of Research Methodology by Alok and Mishra (2017). This means the paper intends to formulate a general theory of achieving compliance with the external requirements of the CRA, as they concern DYNAMO. There are no hard measurable variables, meaning the paper estimates compliance as qualitative values through conceptual research, rather than measurable degrees of compliance with empirical evidence gathering. (Alok, Mishra 2017, p. 3).

As descriptive research is non-experimental, we are focusing on “what” - what are the requirements for CRA compliance that impact DYNAMO (Hassan 2024). While we do provide suggestions and framework plans for achieving compliance and reducing liability for DYNAMO, these are not applied nor experimented with as of the writing of this paper.

These methodology choices were intentional to remain within the confines set by our research plan and ethical foundation; this leaves room for future studies in this field to be completed. Our data was a mix of legal documentation by the EU themselves, and documents written by expert entities describing the impacts, legislation, and difficulties of compliance with CRA. We have used some supplementary sources whose veracity and academic qualities are of a lesser degree – they have been used as supplements to enhance and emphasize our conclusions and justifications for completing this research.

4. Operational Guide for DYNAMO's Compliance with the CRA

Adapting DYNAMO to meet the requirements of the Cyber Resilience Act involves implementing a robust and proactive approach that addresses both technical and administrative aspects of cybersecurity. These measures will ensure that DYNAMO complies with EU regulations, provides safer services to its users, and fosters best cybersecurity practices. The following sections outline the key areas of focus for DYNAMO to achieve compliance, supported by relevant sources.

4.1 Risk Management Frameworks

To comply with CRA requirements, DYNAMO must establish a comprehensive risk management framework. This framework should include regular vulnerability assessments and corrective actions to mitigate identified risks.

Such a system would reduce exposure to known attack surfaces, thereby enhancing the security posture of the platform (ENISA 2024). A systematic approach to risk management is essential for aligning with cybersecurity standards and ensuring long-term resilience. By proactively addressing vulnerabilities, DYNAMO can minimize risks and maintain operational continuity, even in the face of evolving cyber threats (ENISA 2024).

4.2 Collaboration with Third Parties

Effective collaboration with third-party suppliers and service providers is a critical component of CRA compliance. DYNAMO must develop an operational model to ensure that external suppliers and components comply with regulatory requirements. This can be achieved through contractual agreements and regular audit procedures (Shaffique 2024). Third-party compliance is vital for reducing supply chain vulnerabilities and ensuring that all components of a system meet the required security standards. By fostering transparency and accountability within its supply chain, DYNAMO can enhance its overall cybersecurity posture and build trust among its stakeholders (Shaffique 2024).

4.3 Incident Reporting Mechanism

The ability to promptly detect and report cybersecurity incidents is a cornerstone of CRA compliance. DYNAMO must implement an efficient system for incident reporting that enables timely communication with CSIRT networks and ENISA. Organizations are required to report incidents within 24 hours of detection to ensure a swift response and mitigate potential impacts (ENISA 2024). This measure not only enhances user confidence but also demonstrates DYNAMO's commitment to transparency and regulatory compliance (ENISA 2024).

4.4 Utilization of Open-Source Software

The CRA provides specific exemptions for open-source software, which can be leveraged by DYNAMO as part of its risk transference strategy. By integrating open-source solutions such as the Malware Information Sharing Platform (MISP) open-source threat intelligence platform into its framework, DYNAMO can achieve compliance while maintaining flexibility in its development processes (Noël, 2024b). Open-source software offers a lightweight approach to addressing certain regulatory requirements, making it a valuable tool for organizations aiming to reduce operational and compliance burdens (Noël, 2024b).

However, to address potential concerns regarding security and maintenance, it is crucial to include a detailed risk assessment and mitigation strategy for open-source components. This approach ensures that open-source solutions can meet the security and maintenance requirements stipulated by the EU Cyber Resilience Act. By integrating comprehensive risk management practices, organizations can effectively utilize open-source software while maintaining robust security postures. This balanced perspective highlights the benefits of open-source software while acknowledging and addressing the associated risks, thereby aligning with the overarching goals of the EU's cyber resilience framework.

5. Conclusions

This study determines how the DYNAMO platform and tools should be developed to better comply with the Cyber Resilience Act. The result guides the DYNAMO project towards achieving CRA compliance. This WIP aims to understand the relationship between the CRA and DYNAMO, what kind of limitations the CRA would put on the DYNAMO platform and tools, and how to guide the DYNAMO project to its outputs to be CRA compliant. Although extensive research has been conducted on the Cyber Resilience Act itself, no studies have specifically combined the CRA with the DYNAMO project. Therefore, this research aims to fill this gap. Credible sources were utilized, and transparency in source selection was maintained to ensure that the conclusions are replicable.

During the research, several key findings were identified that DYNAMO needs to consider to achieve CRA compliance. DYNAMO must establish a comprehensive risk management framework to ensure that mandatory security standards are met and to enhance the overall credibility of the DYNAMO project. Additionally, DYNAMO must develop an operational model to ensure the compliance of external suppliers and components through contractual agreements and audit procedures. An efficient system must be developed for DYNAMO to enable the prompt detection and reporting of incidents to CSIRT networks and ENISA within 24 hours, as required by the CRA. It was also noted that the CRA exempts open-source software, which should be integrated into DYNAMO's risk transference system.

By implementing these measures, DYNAMO can align its operations with the CRA's stringent requirements and set a benchmark for cybersecurity excellence. Establishing a comprehensive risk management framework, fostering third-party compliance, developing an efficient incident reporting mechanism, and utilizing open-

source software collectively position DYNAMO as a leader in secure digital infrastructure. These steps not only protect users but also strengthen DYNAMO's market position and contribute to the broader adoption of cybersecurity best practices across industries.

Acknowledgements

Acknowledgment 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

Alok, S., Mishra, S.B. 2017. Handbook of Research Methodology. https://www.researchgate.net/publication/319207471_HANDBOOK_OF_RESEARCH_METHOD- OLOGY. Accessed 09.12.2024.

Burri, M., Zihlmann, Z. 2023. "The EU Cyber Resilience Act – An Appraisal and Contextualization." EuZ – Zeitschrift Für Europarecht, doi:10.36862/eiz-euz015. Accessed 16.12.2024.

Chiara, P. 2022a. "The Cyber Resilience Act: The EU Commission's Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements." International Cybersecurity Law Review, vol. 3, no. 2, Nov. 2022, pp. 255–72, doi:10.1365/s43439-022-00067-6.

Chiara, P. 2022b. "The IoT and the New EU Cybersecurity Regulatory Landscape." International Review of Law Computers & Technology, vol. 36, no. 2, May 2022, pp. 118–37, doi:10.1080/13600869.2022.2060468.

DYNAMO 2024. horizon-dynamo.eu. Accessed 23.12.2024.

ENISA 2024. Cyber Resilience Act Requirements Standards Mapping - Joint Research Centre & ENISA Joint Analysis. Accessed 10.10.2024. https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-stand- ards-mapping. Accessed 17.12.2024.

European Commission 2024. Cyber Resilience Act. Accessed 10.12.2024. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act. Accessed 17.12.2024.

Fedienko, O. 2024. "The European Experience of Legislative Support for Strengthening Cyber Resilience." Information and Law, no. 2(49), June 2024, pp. 178–89, doi:10.37750/2616-6798.2024.2(49).306208.

Hassan M. 2024. Research Methodology – Types, Examples and writing Guide. https://researchmethod.net/methodology/ Accessed 09.12.2024.

Hevner, A., March, S., Park, J., & Ram, S. (2004) "Design Science in Information Systems Research", *MIS Quarterly* Vol 28 No 1, pp 80–90.

Noël, D. 2024a. Enabling EU Legislation Compliance with NXP Security Technologies. Powerpoint presentation. https://www.nxp.com/docs/en/training-presentation/TP-TD24-EUF-ENT-T4759.pdf Accessed 10.10.2024.

Noël, D. 2024b. Cybersecurity by Design: Navigating the New CRA Regulations. https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts- new-law-on-security-requirements-for-digital-products/?utm_source=chatgpt.com. Accessed 09.12.2024.

Rosenauer, P., Colonna, V. 2024. A comprehensive guide: Understanding the EU Cyber Resilience Act. PwC insights, https://www.pwc.ch/en/insights/regulation/understanding-the-eu-cyber-resilience-act.html#content-free-1-ea0e Accessed 09.12.2024.

Schmittner, C., Veledar, O., Faschang, T., Macher, G. & Brenner, E. 2024. Fostering Cyber Resilience in Europe: An In-Depth Exploration of the Cyber Resilience Act. Conference paper. Springer Cham. https://doi.org/10.1007/978-3-031-71139-8_26 Accessed 10.10.2024.

Shaffique, M. 2024a. Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark? Computer Law & Security Review. Volume 54. https://doi.org/10.1016/j.clsr.2024.106009. Accessed 13.10.2024.

Shaffique, M. 2024b. The EU Cyber Resilience Act: Implications for IoT Devices. https://www.iotapproval.com/the-eu-cyber-resilience-act-regulation-2024-2847-and-directive-2022-30-a-com- plete-guide-to-compliance/?utm_source=chatgpt.com. Accessed 09.12.2024 .