# Cyber Resilience Under the EU Framework: Insights from an Applied Case Study on Critical Sectors

**Alina-Camelia BELCIU (VASILESCU)[1], Marius PREDA[2]**
[1] Bucharest University of Economic Studies, Bucharest, Romania
belciualina21@stud.ase.ro
[2] Military Technical Academy, Bucharest, Romania
marius.preda@mta.ro

**Abstract**

*The increasing frequency, severity, and complexity of cyber-attacks at EU level highlights the significant importance of robust cyber security frameworks. This article examines the role of EU regulations, in particular the Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) and the Cyber Resilience Act (CRA), in strengthening cyber resilience in critical sectors. First, the review of EU regulations was carried out through a comparative analysis of the legislative documents to highlight objectives, targeted entities, security measures, and compliance and clarify how they are designed to improve cyber resilience in critical sectors. Furthermore, the methodology includes an applied case study designed to explore the practical implications of European regulations on cyber resilience through the examination of the hybrid threat - multiple cyber-attacks mixed with influence operations through the cyberspace targeting the civilian and defense infrastructures of an essential port. By analyzing the attacks through the lens of the NIS 2 Directive and CRA, this case study illustrates how EU regulations provide an efficient foundation for strengthening security and response measures. It also identifies operational challenges and demonstrates how adaptable frameworks aligned with EU regulations enable organizations to recover more effectively. These findings contribute to the broader discourse on securing critical infrastructures and advancing practical solutions to cyber resilience in an interconnected digital environment. To further improve understanding and preparedness, future research should focus on organizing tabletop exercises (TTX) that simulate scenarios similar to those analyzed in this case study.*

**Index terms:** Critical infrastructure, Cyber-attacks, Cyber resilience, Cyber security, EU regulations

**References**


[1]. A. Fleck, "Cybercrime expected to skyrocket in coming years," Statista, 2022. Available: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/. Accessed: Dec. 1, 2024.

[2]. J. Pavão, R. Bastardo, D. Carreira, and N. P. Rocha, "Cyber Resilience, a Survey of Case Studies," Procedia Computer Science, vol. 219, pp. 312-318, 2023, doi: 10.1016/j.procs.2023.01.295. Available: https://www.sciencedirect.com/science/article/pii/S1877050923003034.

[3]. D. A. Sepúlveda Estay, R. Sahay, M. B. Barfod, and C. D. Jensen, "A systematic review of cyber-resilience assessment frameworks," Computers & Security, vol. 97, p. 101996, 2020, doi: 10.1016/j.cose.2020.101996. Available: https://www.sciencedirect.com/science/article/pii/S0167404820302698.

[4]. B. Dupont, C. Shearing, M. Bernier, and R. Leukfeldt, "The tensions of cyber-resilience: From sensemaking to practice," Computers & Security, vol. 132, p. 103372, 2023, doi: 10.1016/j.cose.2023.103372. Available: https://www.sciencedirect.com/science/article/pii/S0167404823002821.

[5]. M. R. Shaffique, "Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark?", Computer Law & Security Review, vol. 54, p. 106009, 2024, doi: 10.1016/j.clsr.2024.106009. Available: https://www.sciencedirect.com/science/article/pii/S0267364924000761.

[6]. S. M. AlHidaifi, M. R. Asghar, and I. S. Ansari, "Towards a Cyber Resilience Quantification Framework (CRQF) for IT infrastructure," Computer Networks, vol. 247, p. 110446, 2024, doi: 10.1016/j.comnet.2024.110446. Available: https://www.sciencedirect.com/science/article/pii/S1389128624002780.

[7]. S. Lyeonov, W. Strielkowski, V. Koibichuk, and S. Drozd, "Impact of Internet and mobile communication on cyber resilience: A multivariate adaptive regression spline modeling approach," International Journal of Critical Infrastructure Protection, vol. 47, p. 100722, 2024, doi: 10.1016/j.ijcip.2024.100722. Available: https://www.sciencedirect.com/science/article/pii/S1874548224000635.

[8]. J. Jeimy and M. Cano, "FLEXI - A Conceptual Model for Enterprise Cyber Resilience," Procedia Computer Science, vol. 219, pp. 11-19, 2023, doi: 10.1016/j.procs.2023.01.258. Available: https://www.sciencedirect.com/science/article/pii/S1877050923002661.

[9]. D. Šehović, "Cyber resilience of financial institutions," Bankarstvo, vol. 46, no. 4, pp. 134-151, 2017. Available: https://www.ceeol.com/search/article-detail?id=908482.

[10]. C. Ciuchi, "Developing a Comprehensive Model for Digital Lifelong Learning Using Cyber Resilience Framework," in Proceedings of the International Conference on Cybersecurity and Cybercrime, pp. 105-112, 2022. Available: https://www.ceeol.com/search/chapter-detail?id=1097199.

[11]. G. A. Hubbard, "State-level Cyber Resilience: A Conceptual Framework," ACIG (Applied Cybersecurity & Internet Governance), vol. 2, no. 1, 2023, doi: 10.60097/ACIG/162859. Available: https://www.ceeol.com/search/article-detail?id=1219159.

[12]. European Commission, EU Cybersecurity Strategy, 2020. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy. Accessed: Oct. 12, 2024.

[13]. European Commission, "Communication on the EU Security Union Strategy," COM/2020/605, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content /EN/TXT/?uri=CELEX:52020DC0605. Accessed: Dec. 1, 2024.

[14]. European Parliament and Council, Regulation (EU) 2016/679 of 27 Apr. 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, "General Data Protection Regulation (GDPR)," OJ L 119, 4 May 2016, pp. 1-88. Available: https://eur-lex.europa.eu/eli/reg/ 2016/679/oj. Accessed: Oct. 10, 2024.

[15]. European Parliament and Council, Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, "NIS Directive," OJ L 194, 19 July 2016, pp. 1-30. Available: http://data.europa.eu/eli/dir/2016/1148/oj. Accessed: Oct. 02, 2024.

[16]. European Parliament and Council, Regulation (EU) 2019/881 of 17 Apr. 2019 on ENISA (the European Union Agency for Cybersecurity) and on ICT cybersecurity certification, "Cybersecurity Act," OJ L 151, 7 June 2019, pp. 15-69. Available: http://data.europa.eu/eli/reg/2019/881/oj. Accessed: Oct. 11, 2024.

[17]. European Parliament and Council, Regulation (EU) 2022/2554 of 14 Dec. 2022 on digital operational resilience for the financial sector, "DORA," OJ L 333, 27 Dec. 2022, pp. 1-79. Available: http://data.europa.eu/eli/reg/2022/2554/oj. Accessed: Oct. 14, 2024.

[18]. European Parliament and Council, Directive (EU) 2022/2557 of 14 Dec. 2022 on the resilience of critical entities, OJ L 333, 27 Dec. 2022, pp. 164-198. Available: http://data.europa.eu/eli/dir/2022/2557/oj. Accessed: Oct. 15, 2024.

[19]. European Parliament and Council, Directive (EU) 2022/2555 of 14 Dec. 2022 on measures for a high common level of cybersecurity across the Union, "NIS 2 Directive," OJ L 333, 27 Dec. 2022, pp. 80-152. Available: http://data.europa.eu/ eli/dir/2022/2555/oj. Accessed: Oct. 13, 2024.

[20]. European Parliament and Council, Regulation (EU) 2024/2847 of 23 Oct. 2024 on horizontal cybersecurity requirements for products with digital elements, "Cyber Resilience Act," OJ L 2847, 20 Nov. 2024. Available: http://data.europa.eu/eli/reg/ 2024/2847/oj. Accessed: Dec. 01, 2024.

[21]. European Commission, The EU Cyber Solidarity Act, 2023. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity. Accessed: Dec. 01, 2024.

[22]. European Parliament and Council, Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence, "AI Act," OJ L 1689, 12 July 2024. Available: http://data.europa.eu/eli/reg/2024/1689/oj. Accessed: Dec. 02, 2024.