Strengthening Collective Cyber-Defence in the EU

29 DECEMBER 2025

Nikoloz Asatiani



Strengthening Collective Cyber Crisis Defence in the EU: Comparing the NIS2 and the Cyber Solidarity Act.

Cyber incidents actively challenge critical services across the European Union. With cascading events that can transcend national borders. Current cyberthreats have made it a type of priority for the EU to introduce a wide array of cybersecurity frameworks. As it is outlined in ENISA's framework, recent assessments indicate a sustained increase in the volume, diversity, and impact of cyber incidents across the EU, with public administration and critical services being among the most affected sectors (European Union

Agency for Cybersecurity [ENISA], 2023, pp. 4–5). The rise of cyber incidents does not only cause issues for the cybersecurity scene but also has significant implications for the entire security scene of the European Union, as they can cause social, economic and even political disruptions (pp. 15–17). The issue becomes especially relevant when considering the cross-border nature of cyber threats revealed by Russia's invasion of Ukraine, which has exposed the EU's dependency on digital infrastructure and the vulnerability of cyberspace to coordinated cyberattacks on critical services (Car, 2025, p. 1).

The recurring issue of cybersecurity vulnerability has brought the European Union to progressively strengthen its cybersecurity and governance frameworks. Acknowledging the fact that fragmented responses are not sufficient in addressing due to the cross-border nature of cyber risks, the EU adopted a set of regulatory instruments that aim to enhance preparedness and resilience towards cyber risks. These two are the Network and Information Security 2 Directive (NIS2) and the Cyber Solidarity Act, enacted in October 2024 and February 2025, respectively.

Together, these frameworks reflect an evolving EU approach that combines national responsibility with emerging collective instruments to address cyber crises more effectively. This brings forth a question. To what extent do the NIS2 and the Cyber Solidarity Act strengthen the EU's capacity for collective cyber crisis defence, and how do their governance designs affect the balance between national and EU-level crisis management?

Conceptual Framework: Collective Crisis Defence

In the broader discipline of security studies, "collective crisis defence" can be defined as a type of coordination among sovereign actors to counter threats that cannot be tackled unilaterally (Deni, 2023, pp. 208–209). Adapted to the cybersecurity domain, collective cyber defence can be understood as a collective ability of multiple states to prepare for and detect large-scale cyber incidents. In the brief, the concept of collective crisis defence is evaluated using two key parameters: baseline national resilience and cross-border response capacity. These parameters were chosen because they capture the two core dimensions of how collective cyber crisis defence operates in practice. Baseline national resilience reflects the extent to which member states are equipped to tackle and prevent cyber incidents before they escalate, while cross-border crisis response capacity is integral to the EU's ability to coordinate action and provide support when incidents exceed national capabilities due to the cross-border nature of cybersecurity threats. Together, these frameworks allow for an assessment of both preventive and reactive elements of collective cyber crisis defence, addressing the "to what extent" dimension of the research.

For the sake of the analysis, the concept of "situational awareness" is treated as an integral element of cross-border crisis response, as early detection and information-sharing are preconditions for effective action during cyber crises.

Context behind the framework: NIS2 (Network and Information Systems 2)

The NIS2 directive was created to address fragmentation in cybersecurity preparedness across member states in order to facilitate resilience of critical cybersecurity sectors. Rather than centralising operational control at the EU level, the NIS2 reinforces responsibility by obliging member states to create supervisory authorities and consistently report incidents to already active monitoring agencies, such as CSIRT **(Computer Security Incident Response Team)** (European Parliament & Council of the European Union, 2022).

The capacity of the NIS2 creates collective cyber resilience by elevating baseline capabilities of EU member states. It introduces mandatory risk management measures, such as incident reporting obligations and supervisory frameworks, that aim to improve preparedness within the member states. At the EU level, coordination is facilitated by large-scale networks such as the CSIRTs network, which supports information exchange, although it does not hold any operational authority within the EU (European Parliament & Council of the European Union, 2022).

Context behind the framework: The Cyber Solidarity Act

The Cyber Solidarity Act is a representation of a shift in EU cybersecurity governance from a focus on baseline resilience to an EU-level preparedness and crisis response. It is specifically designed to address cyber incidents of a cross-border nature that can exceed national capacity. The act tackles the gaps by establishing joint response mechanisms, these being the establishment of a European network of Security Operations Centres, intended to improve shared detection and early warning capabilities, as well as a Cyber Emergency Mechanism and a Cybersecurity Reserve to provide technical assistance to affected Member States (Car, 2025, p. 1).

Unlike the NIS2, the Cyber Solidarity Act does not seek to create baseline cybersecurity standards but instead focuses on EU-level preparedness and support mechanisms during major cyber crises. At the same time, the Act explicitly preserves Member States' primary responsibility for national security, meaning that EU intervention remains supportive and contingent on national consent rather than directive (Car, 2025).

To what extent are the NIS2 and Cyber Solidarity Act applicable mechanisms?

This section will address to what extent the NIS2 and Cyber Solidarity Act strengthen the EU's capacity for collective cyber crisis defence by comparing their governance strategies across two dimensions necessary for proper cyberspace safeguarding: baseline resilience and cross-border crisis response. The analysis focuses on how the policy design choices can affect the collective cybersecurity capacity of the EU.

Baseline resilience

Baseline national resilience refers to the minimum level of preparedness that is required in order to prevent cyber incidents before they occur.

The NIS2 has an indirect role in the creation of a baseline resilience by elevating baseline capacity across EU Member States. This is achieved by creating minimum requirements that states must adhere to, which mitigate systemic vulnerabilities that arise from uneven security capacity (European Parliament & Council of the European Union, 2022).

In contrast, the Cyber Solidarity Act does not create new standards for the EU members to follow regarding baseline resilience. Rather, it suggests the idea of an adequate national baseline and focuses on mobilising preparedness when a certain crisis exceeds the national operational limit for the entirety of the EU. In this sense, the Act fills a gap left by the NIS2 rather than duplicating its function (Car, 2025, pp. 3-5).

This demonstrates a trade-off in the idea of collective cyber crisis defence; the NIS2 enhances stability through national contributions, while the Cyber Solidarity Act relies on already existing national resilience without actively constructing it.

Cross-border crisis response

A key point in the effectiveness of a policy is the ability to address cross-border issues when cyber incidents escalate. This dimension is critical in collective cyber crisis defence, as large-scale incidents often create cascading events that can cause issues for political, economic, and other sectors, as previously outlined by ENISA (2023, pp. 4-5). Cross-border crisis response encompasses both the capacity to coordinate assistance during major cyber incidents and the ability to achieve shared situational awareness across Member States.

While the NIS2 strengthens coordination through reporting obligations and mechanisms such as **EU-CyCLONe**, its cross-border crisis response capacity is limited, since the collective outcomes are highly dependent on the national capabilities of the Member States and their willingness to act (European Parliament & Council of the European Union, 2022, Art. 16). These constraints constitute one of the main drivers for the adoption of the Cyber Solidarity Act, which enhances EU-level coordination, preparedness and response mechanisms (Car, 2025, p. 3).

The Cyber Solidarity Act directly enhances the outlined issue of cross-border crisis response by introducing operational instruments that enhance situational awareness at the Union level through the Cybersecurity Alert System, while simultaneously strengthening response capacity via the establishment of an EU Cybersecurity Reserve (Villani 2025, pp. 491–492). This helps the overall monitoring and structure of the cyber responses. The shift represents an evolution in EU cybersecurity governance in which resilience-oriented, risk-based management is complemented by tools for the anticipation and management of threats (Backman, 2023, pp. 95-96).

Although the Cyber Solidarity Act introduces significant advances in the EU-level crisis response, it also has presented structural and legal limitations that limit its effectiveness as a policy. The Cyber Solidarity Act does not have the ability to replace national cybersecurity systems and still

heavily depends on the willingness of the states to participate during emergencies, which has the potential to hinder a collective response measure (Villani 2025, pp. 494-495). This issue is especially apparent given that EU-level actors operate within institutional constraints characterised by limited enforcement powers, making the idea of international EU-level support more difficult to achieve (Dunn Cavelty & Smeets, 2023).

To summarise, in a cross-border context, the Cyber Solidarity Act strengthens the EU's collective crisis-response capacity by institutionalising joint coordination mechanisms, although the coordination remains constrained by governance arrangements that favour cooperation over an established centralised command system. By contrast, the NIS2 continues to face uneven implementation across Member States and limited EU-level enforcement, as it relies on nationally administered compliance (Eckhardt & Kotovskaia, 2023, p. 155).

Overall Comparative Assessment

Taken together, the comparison suggests that the NIS2 and the Cyber Solidarity Act do strengthen EU collective crisis defence but in complementary and asymmetric ways. The NIS2 primarily functions as a foundational instrument that stabilises collective resilience through responsibility, while the Cyber Solidarity Act expands EU-level preparedness and capacity without diminishing the national authority of states; therefore, collective cyber crisis defence within the EU becomes a layered governance model rather than a singular system. When analysing and creating effective cybersecurity measures, these two acts must be analysed as complementary to their gaps.

The Cyber Solidarity Act should not be seen as a replacement for the established structures that are already in place by the NIS2; rather, it is "an additional instrument to the Computer Security Incident Response Team (CSIRT) network which is provided for by the NIS2 Directive" (Villani 2025, p. 489). It is a complement to the NIS2's established structures while addressing the gaps as previously outlined.

Final Conclusion

This brief analysed the future of the European cyberspace policies and their implications. The question asked to what extent the NIS2 Directive and the Cyber Solidarity Act strengthen the European Union's capacity for collective cyber crisis defence by comparing their effects on baseline national resilience and cross-border crisis response. The analysis showcased that both of the policies contribute to the collective capacities in their own distinct and asymmetric ways. The NIS2 strengthens collective defence indirectly by harmonising national obligations and stabilising baseline resilience, while the Cyber Solidarity Act enhances EU-level preparedness and response capacity when cyber incidents exceed national capabilities.

At the same time, neither instrument has the ability to fundamentally change the distribution of authority in EU cybersecurity governance. The NIS2 remains constrained by uneven national contributions and limited EU-level enforcement, while the Cyber Solidarity Act creates EU-level

solidarity while still having issues with supranational command. As a result, collective cyber crisis defence in the EU has to be regarded with a layered governance model in which national responsibility becomes a top priority but can be complemented by EU-level support mechanisms to take into account the rising importance of cyber warfare preparedness.

Overall, the Cyber Solidarity Act should be understood not as a replacement for the NIS2 but rather as an additional instrument that can help address the gaps left by the NIS2. Together, these frameworks can contribute to the rising advances in cybersecurity.

References

Backman, S. (2023). Risk vs. threat-based cybersecurity: the case of the EU. European Security (London, England), 32(1), 85–103. https://doi.org/10.1080/09662839.2022.2069464

Car, P. (2025). Cyber solidarity act (EU Legislation in Progress briefing, 3rd ed.). European Parliamentary Research Service (EPRS). https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/754614/EPRS_BRI(2023)754614_EN.pdf

Deni, J. R. (2023). Collective defence. In Research Handbook on NATO (pp. 208–221). Edward Elgar Publishing. https://doi.org/10.4337/9781839103391.00026

Dunn Cavelty, M., & Smeets, M. (2023). Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority. Journal of European Public Policy, 30(7), 1330–1352. https://doi.org/10.1080/13501763.2023.2173274

Eckhardt, P., & Kotovskaia, A. (2023). The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive. International Cybersecurity Law Review, 4(2), 147–164. https://doi.org/10.1365/s43439-023-00084-z

European Parliament and the Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union, L 333, 80–152. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02022L2555-20221227

European Union Agency for Cybersecurity. (2023). ENISA Threat Landscape 2023. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

Villani, S. (2025). The Cyber Solidarity Act: Framework and Perspectives for the New EU-Wide Cybersecurity Solidarity Mechanism Under the EU Legal System. European Journal of Risk Regulation, 16(2), 485–497. https://doi.org/10.1017/err.2025.24