European Journal of Risk Regulation (2025), 1–13
doi:10.1017/err.2025.24

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

The Cyber Solidarity Act: Framework and Perspectives for the New EU-Wide Cybersecurity Solidarity Mechanism Under the EU Legal System

Susanna Villani

Department of Legal Studies, University of Bologna, Bologna, Italy
Email: susanna.villani2@unibo.it.

Abstract

Cybersecurity is a concern to be tackled not only by individual States but also by the European Union as a whole. Building on the recent adoption of Regulation (EU) 2025/38, the so-called *Cyber Solidarity Act*, the study intends to analyse the creation of a supranational capacity to prevent and respond to cyber incidents, by answering the following questions: how and to what extent is solidarity concretely declined in the act in question? How do the mechanisms provided for by this act concretely interact with the Member States' prerogatives in the broader security domain?

Keywords: cybersecurity; EU solidarity; national security

I. Introduction

In recent times, the European Union's cybersecurity agency (ENISA) has reported that, throughout the latter part of 2023 and the initial half of 2024, there was a notable escalation in cybersecurity attacks, setting new benchmarks in both the variety and number of incidents, as well as their consequences on public institutions and large companies.[1] These cyber-attacks have targeted Member States' critical infrastructures, as well as EU institutions and bodies, especially in the run-up to the European Parliament elections.

Such an increase in the intensity, sophistication and pervasiveness of attacks, against public and private entities at all levels, confirms that cybersecurity is a concern to be tackled not only by individual Member States but also by the Union as a whole.[2] For the latter, this involves the consolidation of a strategy that is no longer aimed just at helping governmental bodies monitor cybersecurity in their country and exchange information with their counterparts in other Member States. It should also promote common cyber capabilities, operational cooperation and crisis management mechanisms able to react to cyber attacks both at the national and the supranational level.

[1] ENISA, "ENISA Threat Landscape 2024. Global Cybersecurity Challenges and EU Preparedness" (2024) p 6, available at <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024> (last accessed 13 January 2025).

[2] For an overview of the Union's actions and interventions in the field of cybersecurity, A Barrinha and G Christou, "Speaking Sovereignty: The EU in the Cyber Domain" (2022) 31 European Security 356. The relevance of solidarity in the field of cybersecurity has been expressed by the European Parliament, which has called on the Commission to take into account the risk of cyber-attacks against Member State when defining the future modalities for the implementation of the solidarity clause. See, European Parliament, "Resolution on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" (2013/2606(RSP)).

The present work intends to explore the latest developments within the EU legal framework regarding the creation of a supranational capacity to prevent and respond to cyber incidents, whether intentional or not. This constitutes, *inter alia*, a visible expression of European solidarity, as a fundamental principle of the EU legal order,[3] by ensuring a practical and timely contribution to face cyber emergencies. However, dealing with these scenarios at the EU level calls for attention to the prerogatives of Member States set in Article 4(2) TEU, which requires the Union to "respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security."[4] Hence, in the event of large-scale cyber incidents the promotion of supranational cooperation and solidarity should be balanced with the respect for the Member States' national security competences.

Building on the recent adoption of Regulation 2025/38, the so-called *Cyber Solidarity Act*, establishing a supranational mechanism for preventing, preparing for and responding to large-scale cyber threats,[5] the study focuses on two main questions. First, how and to what extent is solidarity concretely declined in the act in question? Second, how do the mechanisms provided for by this act concretely interact with the Member States' prerogatives in the broader security domain?

The structure of the article is as follows. First, it offers a brief overview of the evolution of the EU cybersecurity strategy (Section II). Next, it considers the key features of the *Cyber Solidarity Act*, with particular emphasis on the legal basis and the mechanisms it establishes (Section III). The analysis then explores how solidarity finds concrete expression in the tools set by the Regulation, by underlining their integrative contribution to other solidarity mechanisms at the supranational level (Section IV). Later, particular attention is paid to the interweaving of the Regulation with the dynamics of national security within the EU legal framework by underlining the role of the principle of loyal cooperation as complementary to solidarity in the event of emergencies (Section V). The article will close with reflections on the contribution of the *Cyber Solidarity Act* to the affirmation of a EU-wide cybersecurity system (Section VI).

II. The consolidation of the EU cybersecurity strategy

Even though cybersecurity was included by the European Commission among the Union's priorities as early as 2001,[6] it does not appear as a specific policy area in primary law, nor an explicit legal basis for regulating this sector exists.[7] Over the last decade, however, it has gained new momentum, with the EU institutions adopting legislation on the basis of market interests within the meaning of Article 114 TFEU.[8]

[3] Judgment of the Court of Justice of 7 February 1973, Case C-39/72, *Commission v Italy*; 7 February 1979, Case C-128/78, *Commission v United Kingdom*.

[4] For comments, see, among the others, E Cloots, *National Identity in EU Law* (Oxford, Oxford University Press 2015); L Corrias, "National Identity and European Integration: the Unbearable Lightness of Legal Traditions" (2016) European Papers 383; G Di Federico, "The Potential of Article 4(2) TEU in the Solution of Constitutional Clashes Based on Alleged Violations of National Identity and the Quest for Adequate (Judicial) Standards" (2019) 25 European Public Law 347.

[5] Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act).

[6] European Commission, "Network Security and Information Security: Proposal for a European Strategic Approach" COM(2001) 298 final, 6 June 2001.

[7] GG Fuster and L Jasmontaite, "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights" in M Christen, B Gordijn and M Loi (eds), *The Ethics of Cybersecurity* (Cham, Springer 2020) p 98.

[8] M Varju, "5G Networks, (Cyber)Security Harmonisation and the Internal Market: The Limits of Article 114 TFEU" (2020) European Law Review 471.

In 2013, the Barroso II Commission presented the first *EU Cybersecurity Strategy: An Open and Secure Cyberspace*,[9] aimed to ensure a cyberspace which is accessible to all and, at the same time, equipped with the appropriate tools to guarantee the confidentiality of the data and information contained therein. Since the adoption of this strategy, the Commission led by Juncker proceeded to adopt two key legal instruments.

The first was the Directive on the Security of Network and Information Systems (NIS Directive),[10] which is widely recognised as the first piece of EU legislation on cybersecurity. On the premise that network and information systems play an essential role in facilitating the cross-border movement of goods, services and people,[11] it has introduced specific rules on the exchange of information and the obligation of minimum security requirements for major economic operators providing digital services. The second instrument is Regulation 2019/881 (the so-called *Cybersecurity Act*),[12] which strengthened the role of ENISA established in 2003,[13] and defined a framework for the introduction of a EU certification system for the cybersecurity of products, services and processes.

In 2020 the Commission adopted the new Communication *Shaping Europe's digital future*[14] and, shortly afterwards, the new *Security Union Strategy* for the period 2020–2025,[15] setting out further tools and measures to be developed to ensure the security of both the physical and digital environment. The elements of attention range here from the fight against terrorism to organized crime, passing through the prevention and detection of hybrid threats and the increase in the resilience of critical infrastructures, up to the strengthening of cybersecurity and the promotion of research and innovation.

Following this Communication and the European Council Conclusions,[16] in December 2020 the European Commission and the High Representative for Foreign Affairs presented the new *EU Cybersecurity Strategy for the Digital Decade*,[17] as a trigger for the adoption of new regulatory, policy and investment tools to ensure that everyone can "lead a secure digital life" and to create "a resilient Europe, green and digital" thanks to secure and reliable connectivity tools.

[9] Joint Communication of the European Commission and the High Representative of the Union, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" JOIN(2013) 1 final, 7 January 2013.

[10] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[11] Directive (EU) 2016/1148, recital 3.

[12] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA, the European Union Agency for Cybersecurity, and on cybersecurity certification for information and communication technologies, and repealing Regulation (EU) No 526/2013.

[13] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. The Agency is responsible for assisting the Commission and the Member States by increasing their capacities to prevent, address and respond to network and information security problems, providing them with assistance and advice, and contributing to the overall development of a high level of expertise. In addition, the agency should contribute to promoting and disseminating a new culture of security, so that the issue of cybersecurity is adequately addressed at EU and above all national level, through the preparation of guidelines, the identification of best practices and the organisation of exercises, so as to increase the possibilities of adequately dealing with the risks of cyberspace.

[14] European Commission, "Shaping Europe's Digital Future" COM(2020) 67 final, 19 February 2020.

[15] European Commission, "The EU Security Union Strategy" COM(2020) 605 final, 24 July 2020, point 33.

[16] Conclusions of the Special meeting of the European Council (17–21 July 2020), 21 July 2020.

[17] Joint Communication to the European Parliament and the Council, "The EU Cybersecurity Strategy for the Digital Decade" JOIN(2020) 18 final, Brussels, 16 December 2020. For comments, J Odermatt, "The European Union as a Cybersecurity Actor" in S Blockmans and P Koutrakos (eds), *Research Handbook on EU Common Foreign and Security Policy* (Cheltenham; Northampton, MA, Edward Elgar Publishing 2018) p 359; AP Brandão and I Camisão, "Playing the Market Card: The Commission's Strategy to Shape EU Cybersecurity Policy" (2022) 60 Journal of Common Market Studies 1335, 1345.

As set out in *The Strategic Compass for Security and Defence* approved by the Council in March 2022,[18] the conflict between Russia and Ukraine has then reinforced the need to revise the supranational defence strategy in cyber domain. Thus, following the Council's recommendation on the development of the Union's position on cyber deterrence, in November of the same year the High Representative and the Commission jointly presented the Communication on *The EU's Cyber Defence Policy*.[19] This Communication entails to strengthen the tools for defence cooperation and collaboration between States, to enhance collective situational awareness and early detection capacity and, before that, to act decisively in order to provide the EU with adequate cyber skills capable of developing and managing digital technologies.

In light of these objectives and strategic developments, the new cybersecurity plan has provided for a strengthening of existing tools and the adoption of new ones. In February 2020, the EU institutions worked towards the adoption of Directive 2022/2555 (also known as NIS 2)[20] and of a new Directive on the resilience of critical entities.[21] In addition, a targeted revision of the *Cybersecurity Act* was promoted to strengthen the role of ENISA and the mandatory certification system on IT products.[22] The European Commission then put forward two proposals for Regulations: the *Cyber Resilience Act*, introducing essential security requirements for devices interconnected via the Internet to send and receive data,[23] and the *Cyber Solidarity Act*, establishing an *ad hoc* mechanism for preventing, preparing for and responding to large-scale cyber threats.[24] It is the latter that, being entered into force on 4 February 2025, will be the focus of the following sections.

III. The *Cyber Solidarity Act*: legal basis and mechanisms

Regulation 2025/38 of the European Parliament and of the Council establishes measures to improve the detection of cybersecurity threats and incidents, as well as common preparedness and response to large-scale events. The actions will be supported by funding from the Digital Europe Programme (DEP) of the 2021–2027 Multiannual Financial Framework.[25] In comparison to other acts in the cybersecurity domain, the *Cyber Solidarity Act* is not based on Article 114 TFEU, but has a dual legal basis, namely Article 173(3) and Article 322(1)(a) TFEU. The latter provision, concerning the adoption of measures with financial implications, is essential to allow the instruments illustrated below to benefit from a certain degree of flexibility in relation to budget management.

[18] Council of the European Union, "A Strategic Compass for Security and Defence – For a European Union That Protects Its Citizens, Values and Interests and Contributes to International Peace and Security" (adopted 21 March 2022) available at <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf> (last accessed 10 November 2024).

[19] European Commission and High Representative, "EU Policy on Cyber Defence" JOIN(2022) 49 final, 10 November 2022.

[20] 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).

[21] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

[22] Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2019/881 as regards managed security services.

[23] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

[24] For a first comment, PG Chiara and L Bartoli, "Unveiling EU Cybersecurity Law Turf Battles: The Case of the EU Cyber Solidarity Act Proposal" (19 January 2024) SSRN available at <https://ssrn.com/abstract=4700569> (last accessed 10 November 2024).

[25] Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240.

This is necessary given the unpredictable, exceptional and specific nature of the cyber threat landscape. The other – and most significant – provision concerns the EU's competence in the field of industrial policy. It stipulates that the Union and the Member States must ensure the conditions necessary for the competitiveness of Union industry and the optimal exploitation of industrial potential for innovation, research and technological development.[26]

The choice of this legal basis does not come as a surprise. Indeed, the explanatory memorandum accompanying the proposal makes it clear that the Regulation is also part of the new *Industrial Strategy for Europe*.[27] It is aimed to facilitate the EU industry's ascendance as a global actor in digital technologies, thereby reinforcing the Union's competitive edge in the digital market. This could be achieved by also bolstering the resilience of critical infrastructures that are increasingly vulnerable to cyber threats and incidents due to their reliance on information and communication technologies. It is therefore imperative to implement a structured cybersecurity intervention to increase the resilience of citizens, businesses and entities operating in critical sectors against the growing cybersecurity threats in a context of technological improvement.

To achieve these objectives, the Regulation introduces two tools: a *Cybersecurity Alert System* and a *Cybersecurity Emergency Mechanism*.

The *Cybersecurity Alert System* is a supranational infrastructure that will detect, analyse and process data on cyber threats and incidents in the EU. It will do this through the coordination of national and cross-border cyber hubs.[28]

The national cyber hubs, which are public entities, serve as a reference point and gateway for other public and private organisations at the national level, to collect and analyse information on cybersecurity threats and incidents, and contribute to a cross-border hub.[29] Following a call for expressions of interest, the European Cybersecurity Competence Centre (ECCC) will select a national hub for participating in a joint procurement of tools and infrastructures and receiving a grant for their interventions.[30] It should be noted that, as explicitly stated in recital 33 of the Regulation, it is without prejudice to the compliance by Member States with the obligations under Directive (EU) 2022/2555 that require them to designate or establish one or more cyber crisis management authorities and to ensure that they have adequate resources to carry out their tasks in an effective and efficient manner.

Cross-border cyber hubs shall be constituted as consortia of at least three Member States, each represented by a national hub. These hubs are expected to commit to working together in order to coordinate their cyber threat detection and monitoring activities.[31] This implies for the national hubs participating in a cross-border hub to share relevant information related to cyber threats with each other. To this end, it is beneficial to define the details, including the commitment to exchange a significant amount of data and the conditions thereof, in a consortium agreement specifying the principles for sharing information.[32] It should be noted that the cross-border hub platforms represent an additional instrument to the Computer Security Incident Response Team (CSIRT) network which is provided for by NIS 2 Directive for pooling and sharing data on cybersecurity threats from public and private entities.[33] Indeed, when cross-border hubs obtain information relating to a large-scale, potential or ongoing cybersecurity incident, they

[26] For further information on the Union's industrial policy, D Di Carlo and L Schmitz, "Europe First? The Rise of EU Industrial Policy Promoting and Protecting the Single Market" (2023) Journal of European Public Policy 2063.

[27] European Commission, "A New Industrial Strategy for Europe" COM(2020) 102 final, 10 March 2020.

[28] Cyber Solidarity Act, Art 3.

[29] Cyber Solidarity Act, Art 4.

[30] Cyber Solidarity Act, Art 9.

[31] Cyber Solidarity Act, Art 5.

[32] Cyber Solidarity Act, Art 6.

[33] Directive 2022/2555, Art 10.

shall endeavour to provide the relevant information to the European cyber crisis liaison organisation network ("EU-CyCLONe"),[34] the CSIRT network and the Commission, in view of their respective crisis management roles in accordance with the NIS 2 Directive.[35] However, this complementary action also requires that the *Cybersecurity Alert System* avoids duplication and overlapping, in favour of consistency with the other existing instruments of cyber monitoring.

The *Cybersecurity Emergency Mechanism* provides for a number of interventions to support preparedness, response to, and immediate recovery from significant, large-scale or large-scale-equivalent cybersecurity incidents through mutual assistance actions.[36]

The Mechanism's preparedness actions include the coordinated testing of entities operating in sectors deemed to be of critical importance. The Commission, in consultation with ENISA and the NIS Cooperation Group, shall periodically identify pertinent sectors or subsectors from those enumerated in Annex I of NIS 2 Directive, specifically finance, energy, and healthcare. The entities belonging to these sectors are also eligible to receive financial support for coordinated testing exercises at the Union level. Furthermore, the Mechanism may provide practical support for the monitoring of vulnerabilities and risks, as well as the organisation of exercises and training programmes for entities operating in sectors that are not of high criticality.[37]

In order to facilitate a coordinated response to significant incidents, the Regulation introduces a mechanism of intervention comprising a financial and an operational instrument. The financial support, introduced by the legislator's revision, is intended to provide financial assistance to the Member State offering technical assistance to another Member State affected by a cybersecurity incident.[38] The operational or in-kind instrument is based on a EU Cybersecurity Reserve,[39] which comprises pre-committed incident response services provided by private entities designated as "trusted providers" in accordance with the procurement procedures set forth in Article 17. The aforementioned services may be activated by specific categories of "users" including Member States' cyber crisis management authorities, CSIRTs, and Union institutions, bodies, and agencies through the Computer Emergency Response Team (CERT-EU), as established by Regulation 2023/2841.[40] Third countries may also be designated as "users" and thus request support in cases where such provisions are outlined in the association agreements concluded in relation to their participation in the Digital Europe Programme.[41]

Following an incident notification, as also referred to in the Directive 2022/2555, and upon request of the national authorities, the European Commission is tasked with evaluating it and determining whether intervention is necessary.[42] The Commission may, at its discretion, delegate the full or partial management of the operation and administration of the reserve to ENISA.[43] For obtaining operational support, users are required to implement measures designed to mitigate the effects of the incident in

[34] EU-CyCLONe is a cooperation network for Member States national authorities in charge of cyber crisis management. Launched in 2020, it has been formalised in Art 16 of the NIS 2 Directive.

[35] Cyber Solidarity Act, Art 7.

[36] Cyber Solidarity Act, Art 10.

[37] Cyber Solidarity Act, Art 12.

[38] Cyber Solidarity Act, Art 18.

[39] Cyber Solidarity Act, Art 14.

[40] Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, Art 13.

[41] Cyber Solidarity Act, Art 19. Apart from Iceland, Norway and Liechtenstein belonging to the European Economic Area, Albania, Bosnia and Herzegovina, Kosovo, Moldova, Montenegro, Norh Macedonia, Serbia, Turkey and Ukraine have recently conclude agreements for joining the DEP.

[42] Cyber Solidarity Act, Arts 15–16.

[43] Cyber Solidarity Act, Art 14.

question. This includes the provision of direct technical assistance and other resources intended to facilitate incident response and immediate recovery efforts. It is important to note that, following the amendments adopted by the legislator, support from the reserve may also extend to the recovery phase, but is limited to the initial stage of restoring the basic functionalities of the systems.[44]

In order to complete the picture, it is also pertinent to mention the establishment of the *Cybersecurity Incident Review Mechanism*, designed to assess significant cyberattacks with large-scale impacts, identify key lessons, and, if necessary, issue recommendations to enhance the EU's resilience.[45] In response to a request from the Commission or EU-CyCLONe, ENISA is obliged to submit a report that includes lessons learned and recommendations aimed at enhancing the Union's cyber response. In the event that an incident has an impact on a DEP-associated third country, ENISA shall also share the report with the Council and the High Representative for Foreign Affairs.

IV. Lines of solidarity in Union's response to cyber emergencies

The *Cyber Solidarity Act* establishes mechanisms to enhance collective preparedness and response to large-scale cybersecurity incidents, reflecting the EU's comprehensive solidarity framework, which is currently being developed for activation in emergency situations.[46] This section is, therefore, devoted to examine the extent to which, and the forms in which, solidarity is effectively integrated into the provisions of Regulation 2025/38.

As of the *Cybersecurity Alert System*, the establishment of a pan-European infrastructure based on Cyber Hubs, subsidised by the Union through the Digital Europe Programme, has two principal objectives which meet solidarity arguments in the preparedness phase. Firstly, it is intended to enhance the capacity of public authorities to be prepared to potential cyber threats in a timely and effective manner. Secondly, it is designed to strengthen the information exchange system regarding cyber threats, vulnerabilities, attack detection procedures, and cybersecurity alerts among public authorities. Such enhanced coordination and collaboration in the detection, analysis, and processing of data pertaining to cyber threats and incidents across the EU are intended to achieve a unified and concrete goal: safeguarding the cybersecurity interests of the Union and of its Member States. Consequently, this instrument, supported by the principle of loyal cooperation between authorised entities, has the potential to result in *de facto* solidarity, thereby facilitating the pursuit of a common and even supranational interest.[47]

The *Cybersecurity Emergency Mechanism* is the instrument that is explicitly and precisely designed to facilitate solidarity interventions in emergency contexts. In view of the heightened risks and the growing number of cyber incidents affecting Member States, this mechanism has been established "to support the improvement of the Union's resilience to cyber threats and the preparation for and mitigation of, *in a spirit of solidarity*, the

[44] Cyber Solidarity Act, Art 15.

[45] Cyber Solidarity Act, Art 21.

[46] S Blockmans, "L'Union fait la Force: Making the Most of the Solidarity Clause (Art 222 TFEU)" in I Govaere and S Poli (eds), *EU Management of Global Emergencies. Legal Framework for Combating Threats and Crises* (Leiden, Brill 2014) p 111; E Tsourdi, "Solidarity at Work? The Prevalence of Emergency-Driven Solidarity in the Administrative Governance of the Common European Asylum System" (2017) Maastricht Journal of European and Comparative Law 667; A Biondi, E Dagilyté and E Küçük (eds), *Solidarity in EU Law. Legal principle in the Making* (Cheltenham; Northampton, MA, Edward Elgar 2018).

[47] Solidarity as instrument for achieving the supranational common interest has been suggested by the Court of Justice in a number of past judgments: Case C-11/69 *Commission v France*, 10 December 1969; Case C-77/77 *Benzine en Petroleum Handelsmaatschappij BV and Others v Commission of the European Communities*, 29 June 1978; Opinion 1/75, 11 November 1975; Joined Cases C-154/78, C-205/78, C-206/78, C-226/78, C-227/78, C-228/78, C-263/78, C-264/78, C-39/79, C-31/79, C-83/79 and C-85/79 *SpA Ferriera Valsabbia and Others v Commission*, 7 July 1980.

short-term impact of significant cybersecurity incidents, large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents" [emphasis added].[48]

Such a spirit of solidarity is reflected, on the one hand, in the traditional financial support for technical assistance from one Member State to another Member State, as outlined in Article 18 of the Regulation 2025/38, and, in the other one, in the activation of a reserve composed of pre-committed resources. Indeed, the adoption of direct financial support measures is the most traditional way of ensuring an immediate and tangible manifestation of solidarity, by giving the national authorities full responsibility and autonomy in the management of financial resources. Instead, the pre-commitment of resources serves to complement the existing assets of Member States, thereby ensuring greater accessibility and faster deployment of intervention teams. Furthermore, it prevents the duplication of efforts within the Union and its Member States, by requiring a high degree of coordination between the subjects involved. Consequently, solidarity is manifested in the in-kind nature and temporal (that is pre-committed) nature of the Cybersecurity Reserve, thereby enabling a rapid, efficient, and effective response to offensive actions through joint technical and operational interventions conducted within the emergency mechanism.

In practice, if the *Cyber Solidarity Act* had already existed, it could have helped react to the SolarWinds attack in 2020, which affected multiple EU-based entities by highlighting the need for a more unified and rapid response.[49] In that event, the *Cybersecurity Emergency Mechanism* could have been activated to swiftly deploy resources, thereby enhancing both the speed and coordination of the EU's response. The establishment of a shared reserve of resources, along with the mobilisation of certified private-sector providers, would have served to mitigate the impact on critical infrastructure, whilst ensuring a more coherent approach across Member States. The SolarWinds incident thus underscores the importance of the solidarity-based interventions envisaged by Regulation 2025/38, which are designed to protect both Member States and the Union as a whole from large-scale cyber incidents.

Besides these considerations, the operational relevance of solidarity is further emphasised in Article 20 of Regulation 2025/38, which mentions the potential supplementary contribution of the *Cybersecurity Emergency Mechanism* to other existing assistance instruments.

In the first place, it could serve to reinforce the Union Civil Protection Mechanism (UCPM)[50] in the event of a significant cybersecurity incident resulting from or occurring during a natural or man-made disaster on the territory of a State. In the abstract, while the UCPM can intervene to coordinate rescue and humanitarian assistance in the event of an emergency, the *Cybersecurity Emergency Mechanism* could integrate it by mitigating and resolving the (potential) resulting cyber impacts. In this respect, it has to be said that the Cybersecurity Reserve could currently work even better than the model proposed by the UCPM. Indeed, the EU's rapid response capabilities established under the UCPM consist of pre-committed reserves that are rented, leased or owned by Member States; any activation

[48] Cyber Solidarity Act, Art 10(1).

[49] A Coco, T Dias and T van Benthem, "Illegal: The SolarWinds Hack under International Law" (2022) European Journal of International Law 1275.

[50] The EU Civil Protection Mechanism is a system set up in 2001 to coordinate rescue and humanitarian assistance in the event of natural or man-made disasters whose scale or nature exceeds the response capacity of the affected country. The assistance provided by the UCPM consists, in particular, of directing specialised and adequately equipped rescue teams (modules) to interventions and providing material and expert support. Originally set up in 2001, the UCPM was improved in 2013 (Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism) and revised in 2019 (Decision (EU) 2019/420 of the European Parliament and of the Council of 13 March 2019 amending Decision No 1313/2013/EU on a Union Civil Protection Mechanism) and in 2020 (Regulation (EU) 2021/836 of the European Parliament and of the Council of 20 May 2021 amending Decision No 1313/2013/EU on a Union Civil Protection Mechanism).

must therefore be confirmed by them.[51] Instead, the cyber mechanism relies on trusted private sector service providers, certified according to the EU certification scheme, pre-procured through a supranational process and mobilised by the Commission (or ENISA). The fact that these supranational bodies are responsible for deciding on the procurement and deployment of the reserve makes the Union independent of the discretion of national authorities during the activation phase. It could also be argued that, by virtue of their independence from the national authorities and their direct link with the Commission, the Cybersecurity Reserve can ensure greater solidarity on the part of the Union in the event of major or widespread incidents.

Secondly, Regulation 2025/38 suggests that the activation of the emergency mechanism may serve to complement those instruments which implement primary law provisions setting obligations of solidarity typically upon Member States, namely the mutual defence clause (Article 42(7) TEU)[52] and the solidarity clause (Article 222 TFEU).[53]

The mutual defence clause essentially requires Member States to provide aid and assistance by all available means in the event of armed aggression. In such an eventuality, the activation of the *Cybersecurity Emergency Mechanism* would enable the Union to extend support to the Member State that has been the victim of an attack, thereby complementing the efforts of the other Member States under Article 42(7) TEU. Clearly, this intervention requires that the cyber attack is qualified as an armed aggression under international law.[54]

Concurrently, the solidarity clause imposes an explicit and general obligation upon the Union and its Member States to act jointly for assisting a Member State victim of a terrorist attack or of a natural or man-made disaster. It explicitly requires the Union to deploy all available instruments with the objective of providing support to affected Member State(s) and fostering positive synergies among them when a terrorist attack or a natural or man-made disaster occurs. Consequently, despite the solidarity clause is conceived as a last-resort instrument,[55] in the event of its invocation the *Cybersecurity Emergency Mechanism* should be mandatorily activated, thereby obliging the Commission to activate the requisite assets, in particular the reserve, for which it bears responsibility.

Ultimately, in light of the potential for responding to both intentional and unintentional cyberattacks, the mechanisms established by the *Cyber Solidarity Act* have the capacity to serve as a valuable complement to the interventions of preparedness and assistance provided by Member States and also as a means of independent Union intervention in favour of them. Consequently, the Union is not merely a nexus of "solidary integration" between Member States; it also assumes an active role in cybersecurity, thereby establishing the EU level as a unified and distinctive sphere of solidarity.

[51] Regulation 2019/420, Art 12(3).

[52] NIM Nováky, "The Invocation of the European Union's Mutual Assistance Clause: A Call for Enforced Solidarity" (2017) European Foreign Affairs Review 357; T Ramopoulos, "Article 42 TEU" in M Kellerbauer, M Klamert and J Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (Oxford, Oxford University Press 2019) p 276.

[53] For deeper and critical insights on the "solidarity clause," see S Blockmans, "L'Union fait la Force: Making the Most of the Solidarity Clause (Article 222 TFEU)" in I Govaere and S Poli (eds), *EU Management of Global Emergencies* (Leiden, Brill 2014) p 111; P Hilpold, "Filling a Buzzword with Life: The Implementation of the Solidarity Clause in Article 222 TFEU" (2014) Legal Issues of Economic Integration 209; S Villani, *The Concept of Solidarity within EU Disaster Response Law. A Legal Assessment* (Bologna, Bononia University Press 2021) p 199.

[54] F Delerue, "The Threshold of Cyber Warfare: from Use of Cyber Force to Cyber Armed Attack" in *Cyber Operations and International Law* (Cambridge, Cambridge University Press 2020) p 273; I Kilovaty, "Cyber Conflict and the Thresholds of War" in DL Sloss (ed), *Is the International Legal Order Unraveling?* (Oxford, Oxford University Press 2022) p 251.

[55] Council Decision of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause.

V. Balancing solidarity and national security in the cyber domain

The "national identity clause" set out in Article 4(2) TEU[56] establishes that in case of a threat to national security resulting from an emergency or external attack, national authorities have the full responsibility for reacting and protecting those concerned. Consequently, as the affected States are permitted a considerable degree of discretion during the response phase, the implementation of measures at the supranational level is contingent upon the approval and full involvement of national authorities. This rationale, inherent to the State as a sovereign entity, also extends to the cyber domain. Indeed, the possibility of cyber threats causing disruption to essential functions and services is considerable and may result in significant inefficiencies within a State's territory and potentially affect the protection of individuals' fundamental rights.

In light of the aforementioned considerations, the 2024 Council Conclusions on the *Future of Cybersecurity: Implement and Protect Together* emphasised that Member States keep the primary responsibility for responding to large-scale cyber incidents, which have the potential to threaten national security.[57] Moreover, in instances where these incidents may have an international dimension and may necessitate action at the supranational level, such action must be coordinated with national interventions. The aforementioned perspective is also evident in the *Cyber Solidarity Act*, which aims to enhance collective preparedness and response measures against cyber incidents and attacks. The present section is therefore devoted to exploring how the prerogatives of Member States in responding to cyber events are envisaged in the Regulation in question, and whether these prerogatives may in some way compromise the solidarity measures previously illustrated.

From a theoretical standpoint, the necessity to respect Member States' prerogatives in the security domain arises from the choice of Article 173(3) TFEU as the legal basis. This provision, in fact, pertains to a supporting and coordinating competence, which – under Article 2(5) TFEU – precludes the enactment of harmonisation measures and enables the Union to act without superseding the competences of Member States. As explicitly stated in Article 1(4) of the *Cyber Solidarity Act*, "the actions under this Regulation shall be conducted with due respect to the Member States' competences." Moreover, the Regulation underscores the significance of upholding the "essential functions" of the Member States, which encompasses the safeguarding of territorial integrity, the maintenance of law and order, and the protection of national security. In particular, it reaffirms that national security remains the sole responsibility of each Member State.[58]

To recall this constraint, Regulation 2025/38 includes three specific "non-affectation clauses" that have been designed and then reinforced by the legislator to emphasise the necessity of respecting the States' prerogatives in matters of national cybersecurity.

In the first place, the Regulation underlines the voluntary nature of Member States' involvement in the *Cybersecurity Alert System*, as well as the supplementary function of the *Cybersecurity Emergency Mechanism* in relation to States' endeavours to prepare for, respond to and recover from cybersecurity incidents.[59] It implies that the Union's intervention shall necessarily be subordinated to the affected States' willingness. Secondly, following

[56] B Guastaferro, "Sincere Cooperation and Respect for National Identities" in R Schütze and T Tridimas (eds), *Oxford Principles of European Union Law – The European Union Legal Order* (Oxford, Oxford University Press 2018); HJ Blanke, "Article 4: The Relations Between the EU and the Member States" in HJ Blanke and S Mangiameli (eds), *The Treaty on European Union (TEU)* (Heidelberg, Springer 2013) p 229; AS Arnaiz and CA Llivina (eds), *National Constitutional Identity and European Integration* (Cambridge, Cambridge University Press 2013); E Cloots, *National Identity in EU Law* (Oxford, Oxford University Press 2015).

[57] Council of the European Union, *Conclusions on the Future of Cybersecurity: Implement and Protect Together* (adopted 21 May 2024) available at <https://data.consilium.europa.eu/doc/document/ST-10133-2024-INIT/en/pdf> (last accessed 15 November 2024).

[58] Cyber Solidarity Act, Art 1(5).

[59] Cyber Solidarity Act, Arts 3 and 12.

the political agreement reached between the Council and the European Parliament, it is imagined that Member States may assume a role in the establishment of the reserve by interacting with the Commission on the formulation of criteria for tender calls and the procurement procedure for the reserve.[60] Thirdly, there is an emphasis on the limits for the dissemination and disclosure of information: under Article 1(6) of the Regulation, the exchange of confidential information must be limited to what is relevant and proportionate to the final purpose, without affecting the essential national security, public security, or defence interests of Member States. This formulation appears perfectly consistent with Article 346(1)(a) TFEU, otherwise known as the "national defence privilege clause," according to which no Member State shall be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security.[61]

In light of this reconstruction, although the Commission is responsible for activating the Cybersecurity Reserve, the instruments established by the *Cyber Solidarity Act* cannot be designed to replace or radically transform the national cybersecurity systems. The concept of supranational solidarity is thus mitigated by national security arguments. Indeed, the efficacy of the solidarity mechanisms is dependant upon the discretion and willingness of the affected Member States to engage and share information in the event of a cyber emergency. As is often the case in the EU landscape, the solidarity measures that the Union can activate in emergency situations are still bound by the sovereignty of the Member States.

At this juncture, it is clearly premature to speculate on the full scope of the *Cyber Solidarity Act*; however, it is evident that the current structure may encounter issues and frictions with the prerogatives of Member States, thus curtailing the positive effects of the act. Nevertheless, it should be noted that the "national identity clause" cannot derogate the general obligation of Member States to exercise their prerogatives in compliance with EU law. This obligation is derived from the principles that govern the relationship between the Union and the Member States, as set forth in Article 4 TEU, including that of sincere cooperation.[62] With respect to the topic at hand, this principle is relevant insofar as it establishes the duty on the Member States to assist EU institutions and facilitate their actions in carrying out EU tasks, as well as the obligation to refrain from implementing measures that could potentially compromise the attainment of EU objectives. Hence, the principle of loyal cooperation serves to strike a balance between the respect for the authority of Member States in the management of national (cyber) security and the broader imperative of upholding EU law and pursuing actions that align with the common interest and solidarity objectives.[63] Ultimately, it is essential the development of a pluralistic approach that brings the supranational constitutional framework into dialogue with that of the Member States.[64]

By characterising cybersecurity as a matter of general interest at the EU level, the principle of loyalty in conjunction with that of solidarity may prompt Member States to align their national security measures with the EU's solidarity goals. This would ensure that the efforts to protect national interests do not impinge upon collective security objectives. Such alignment could encourage both the Member States and the Union to develop more effective cyber crisis management instruments and foster a more unified response to cyber threats, thereby reinforcing the solidarity between Member States and the EU.

[60] Cyber Solidarity Act, Art 17(3).

[61] For details, see S Peers, "National Security and European Law" (1995) Yearbook of European Law 363; AJ Cornell, "The National Security Challenge to EU Legal Integration" in AB Engelbrekt and X Groussot (eds), *The Future of Europe. Political and Legal Integration Beyond Brexit* (London, Bloomsbury 2019) p 151.

[62] M Klamert, *The Principle of Loyalty in EU Law* (Oxford, Oxford University Press 2014).

[63] F Casolari, *Leale cooperazione tra Stati membri e Unione Europea. Studio sulla partecipazione all'Unione al tempo delle crisi* (Napoli, Editoriale Scientifica 2020) p 207.

[64] A Von Bogdandy and S Schill, "Overcoming Absolute Primacy: Respect for National Identity Under the Lisbon Treaty" (2011) Common Market Law Review 1417, 1452.

VI. Conclusive remarks

In light of the most recent statistics on cyber attacks, which indicate that ransomware, fileless attacks, and phishing remain the primary threats, it is evident that cybersecurity preparedness and a shared response capacity are of paramount importance in order to reduce the risks of network or data compromises. In recent years, the EU has implemented measures to enhance the protection of critical infrastructures and the resilience of the entities operating in this domain, with the objective of avoiding or mitigating the impact of disruptions to essential services.

The current EU cybersecurity strategy can be anchored to the concept of "EU digital (or technological) sovereignty," mentioned for the first time by the President of the European Commission in the State of the Union Address in 2020.[65] Such reading of supranational sovereignty enshrines, *inter alia*, the attempt to extend the parameters of the EU constitutional design to cyberspace,[66] justifying the attribution to the supranational level of powers and instruments to encourage the implementation of regulatory interventions in several sectors to defend the constitutional structure of the Union as a whole from exogenous influences. And, in effect, the EU cybersecurity strategy underpins the need to affirm and protect the value system under Article 2 TEU at the basis of the EU identity in the cyber domain,[67] by highlighting the intertwining of cybersecurity and the security of democratic systems, fundamental rights and the rule of law.[68] The overarching approach of the EU is therefore projected to address current and future online and offline risks, and by equipping itself with robust tools and resources according to the *EU Security Union Strategy*. It is of the utmost importance for the Union to maintain its competitive advantage and protect its digital infrastructure from evolving threats.

In this context, the *Cyber Solidarity Act* represents the most recent regulatory milestone in the development of the comprehensive cybersecurity strategy. It serves to complement the existing legal instruments designed to enhance resilience against cyber threats, thereby ensuring that citizens and businesses can rely on the integrity and reliability of digital technologies. In this regard, the analysis presented in this article leads to two key conclusive considerations, that will need to be verified on the basis of future practice.

Firstly, Regulation 20025/38 provides a comprehensive framework that may support national authorities and enhance solidarity across Member States. This is achieved by establishing a supranational system of preparedness and assistance, which is designed to address particularly serious situations. The principle of solidarity, coupled with that of loyal cooperation envisaged in the EU legal framework, underpins the entire cycle of managing a cyber emergency by requiring Member States to cooperate with each other in

[65] For insights, see L Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU" (2020) Philosophy & Technology 369; S Poli, "Reinforcing Europe's Technological Sovereignty Through Trade Measures: The EU and Member States' Shared Sovereignty" (2023) 8 European Papers 429.

[66] G De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge, Cambridge University Press 2022).

[67] The contours of the constitutional identity of the Union, based on the values referred to in Art 2 TEU as already identified in Opinion 2/13 on the EU's accession to the European Convention on Human Rights, emerged clearly in the twin judgments rendered by the Court of Justice in February 2022 (Case C-156/21 *Hungary v Parliament and Council*, 16 February 2022; Case C-157/21 *Poland v Parliament and Council*, 16 February 2022). For comments, PS Pohjankoski, "The Unveiling of EU's Constitutional Identity – Judgments in C-156/21, *Hungary v Parliament and Council* and C-157/21, *Poland v Parliament and Council*" (2022) *EU Law Live – Weekend Edition*; A Festa, "The 'Twin' Judgments of 16 February 2022: Beyond the Question of Legitimacy, a 'Manifesto' on the Foundations of European Law" (2022) Papers of European Law 81; G Contaldi, "The Judgments of the Court of Justice on the Appeals of Poland and Hungary and the Emergence of the Concept of European Identity" in G Contaldi and R Cisotta (eds), *Courts, Values and European Identity* (Milan, Eurojus 2022) p 87.

[68] GG Fuster and L Jasmontaite, "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights" in M Christen, B Gordijn and M Loi (eds), *The Ethics of Cybersecurity* (Cham, Springer 2020) p 98.

a spirit of loyalty and the Union to activate the *Cybersecurity Emergency Mechanism* when necessary. Hence, the solidarity protection network established by the *Cyber Solidarity Act* has the potential to expand the articulated regulatory ecosystem of cybersecurity measures by providing support for the actions of Member States. Furthermore, when viewed in a broader context, this Regulation is embedded within the already extensive regulatory framework for emergency management, which encompasses a multitude of situations resulting from natural or man-made disasters. So, while Member States' national security prerogatives remain solid, the urgency of a collective response to cyber threats is beginning to challenge the traditional boundaries of this exclusive competence. Indeed, in the event of a particularly significant cyber emergency, both national authorities and the Union bear responsibility for responding and protecting against cyber threats.

Secondly, it is important to note that the support outlined in Regulation 2025/38 is not exclusive to Member States or third countries. It also extends to EU institutions and bodies, enabling them to request assistance from the *Cybersecurity Emergency Mechanism* in the event of a significant cyber incident that could potentially impact EU infrastructure, institutions and, more broadly, the supranational democratic system. The reserve thus may be activated in the event of a hybrid threat targeting the electoral process of the European Parliament or seeking to gain access to EU confidential and classified documents, as well as sensitive non-classified information. In such instances, the Regulation permits a single EU institution, body, office, or agency to request action from the Commission or ENISA, thereby ensuring a prompt response to safeguard the Union's interests. The extension of the Regulation's scope to include EU institutions is a distinctive feature of the regulatory landscape for emergency responses, with notable implications for the EU constitutional dimension. This approach reflects the evolving nature of the threats faced by the Union, highlighting the importance of having its own cybersecurity measures in place alongside those of the Member States.

In light of the potential for cyber attacks to compromise the fundamental infrastructures and democratic systems that underpin the EU's identity, it must rely on instruments, like the reserve of the *Cyber Emergency Mechanism*, that are able to protect its values and constitutional framework. Furthermore, it is important to emphasise that the *Cyber Solidarity Act* outlines an EU sovereignty that operates parallel to, rather than replacing, Member States' sovereignty. Ultimately, it can be stated that the Regulation may contribute to the progressive realisation of the EU's technological sovereignty in the field of cybersecurity, based on the fundamental value of solidarity. Nevertheless, it will be crucial to monitor the intertwining of the EU and Member States' prerogatives in the protection of (supra)national security and sovereignty in the context of forthcoming legal developments in the cyber domain.

Acknowledgment. Research partially funded by the PNRR programme – M4C2 – Investment 1.3, Extended Partnership PE00000013 – "FAIR – Future Artificial Intelligence Research" – Spoke 8 "Pervasive AI," funded by the European Commission under the NextGeneration EU Programme.

Cite this article: S Villani, "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*. https://doi.org/10.1017/err.2025.24