INTERSECT POLICY BRIEF 2

CYBER SOLIDARITY ACT PROPOSAL

Date 20/10/2023

Authors Suzanne Nusselder

Pratham Ajmera

Publication

Tilburg Institute for Law, Technology, and Society (TILT)
www.tilt.nl

INTERSECT is funded by the National Research Council (Grant no. NWA.1160.18.301)

Contact

Suzanne Nusselder
S.C.Nusselder@tilburguniversity.edu

Pratham Ajmera
P.Ajmera@tilburguniversity.edu

1 The Reason Behind The Proposal

In April 2023, the European Commission put forth a proposal for the Cyber Solidarity Act.[1] The Cyber Solidarity Act aims to strengthen the capacity to detect, prepare for, and respond to cybersecurity threats and incidents in the EU.[2]

Although the proposal of the Cyber Solidarity Act has been accelerated by Russia's military aggression towards Ukraine, the proposition of such legislation was, at least in part, already foreshadowed in earlier policy documents.[3] The creation of a European Cyber Shield, a pan-European network of national and cross-border Security Operations Centres (SOCs), which is one of the three key objectives of the Cyber Solidarity Act proposal, has previously been announced in the 2020 Cybersecurity Strategy.[4] However, Russia's military aggression towards Ukraine, which was preceded and accompanied by hostile cyber operations, was considered a game changer and a call for urgent action to enhance the EU's collective cybersecurity crisis management preparedness.[5] The Cyber Solidarity Act proposal delivers on the commitments set out in the Joint Cyber Defence Communication[6] as well as addresses lessons learned from the cyber dimension of the war in Ukraine.[7]

The threat of malicious behaviour in cyberspace goes beyond Russia and is likely to persist. The risk of possible large-scale cyber incidents causing significant disruption or damage to critical infrastructures stems from both state and non-state actors.[8]

With the ever-increasing reliance on information and communication technologies by both the public and the private sector, the exposure to cybersecurity incidents is continuously rising. This growing number of cyberattacks progressively includes supply chain attacks and cyberattacks targeting critical infrastructure. Importantly, cybersecurity incidents can rapidly spill over across borders, sectors, and products. Significant cybersecurity incidents can be too disruptive for one or several affected member states to handle by themselves. Therefore, the Commission considered common action and cooperation at the EU level as essential.[9] To achieve this, the Cyber Solidarity Act aims to increase EU-wide cooperation in preparation for and response to major cyberattacks by implementing the following actions, which the following part explores in detail:

- Deploying a pan-European infrastructure of SOCs (European Cyber Shield) to build and enhance common detection and situational awareness capabilities.
- Creating a Cyber Emergency Mechanism to support Member States in preparing for, responding to and immediate recovery from significant and large-scale cybersecurity incidents.
- Establishing a European Cybersecurity Incident Review Mechanism to review and assess specific significant or large-scale incidents. [10]

[1] Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, COM(2023) 209 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023PC0209 (Hereafter, Cyber Solidarity Act proposal).
[2] Article 1(1), Cyber Solidarity Act proposal.
[3] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, OJ L 239/36; European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council, 'The EU's Cybersecurity Strategy for the Digital Decade', JOIN(2020) 18 final.
[4] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council, 'The EU's Cybersecurity Strategy for the Digital Decade', JOIN(2020) 18 final, p6.
[5] Section 1, Explanatory Memorandum for the proposed Cyber Solidarity Act, COM(2023) 209 final, Page 1.
[6] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council, 'EU Policy on Cyber Defence', JOIN(2022) 49 final.
[7] Stéphane Duguin and Pavlina Pavlova, 'The Role of Cyber in the Russian War against Ukraine: Its Impact and the Consequences for the Future of Armed Conflict' (European Parliament, Directorate-General for External Policies 2023) EP/EXPO/A/COMMITTEE/FWC/2019-01/Lot4/1/C/20, available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf.
[8] Section 1, Explanatory Memorandum for the proposed Cyber Solidarity Act, COM(2023) 209 final, Page 1.
[9] Section 1, Explanatory Memorandum for the proposed Cyber Solidarity Act, COM(2023) 209 final, Page 1.
[10] Article 1, Cyber Solidarity Act Proposal.

2 A Closer Look At The Proposal

General Resilience – The European Cyber Shield:
Chapter 2 of the Cyber Solidarity Act Proposal provides for the establishment and operation of the "European Cyber Shield". Described as an 'interconnected pan-European infrastructure,' comprised on National and Cross-Border Security Operations Centres (National SOCs and Cross-border SOCs respectively).[11] The Cyber Shield collects threat and incident data, out of which it produces actionable information, improves threat detection and situational awareness, and contributes to the development of innovative cybersecurity tools.[12] It is planned to be funded under the Digital Europe Programme,[13] under its Specific Objective 3 (Cybersecurity and Trust).

National SOCs are to be designated by Member States, with each Member State designating at least one, and they must be public bodies. Their function is to act as repositories of cybersecurity related information that can be relied upon by public and private bodies in the concerned Member State as well as being a contributor to any Cross-Border SOCs they may be part of.[14] The acquisition and operation of the tools and infrastructures used by the National SOC are to be bankrolled by the Union and the concerned Member State 50-50. Funding for operating these tools may also be received through grants by the European Cybersecurity Competence Centre (ECCC), provided the National SOC is selected by the ECCC after an expression of interest and participates in a Cross-Border SOC within two years of acquiring said tools and infrastructure[15]

A Cross-Border SOC must be established by at least three Member States through their respective National SOCs. A Cross-Border SOC may also receive grants by the ECCC for operation of the tools and infrastructure it employs. Acquisition of tools and infrastructure are to be funded by the Union and the Member States in the ratio of 75-25, and operation in the ratio of 50-50.[16] Cross-Border SOCs must also engage in information sharing activities among themselves and with Union entities such as European Cyber Crisis Liaison Organisation Network (EU-CyCLONe), Computer Security Incident Response Teams (CSIRT) networks and the European Commission, the procedures and interoperability conditions for which may be prescribed through implementing acts adopted in accordance with the examination procedure[17] in the Cyber Solidarity Act Proposal.[18] Resilience of the Cyber Shield itself must also be provided for by Member States, so that the Shield infrastructure itself (and the data being exchanged through it) does not fall prey to cybersecurity threats.[19]

Resilience on threats and during incidents – The Cyber Emergency Mechanism
Chapter 3 of the Cyber Solidarity Act Proposal establishes the Cyber Emergency Mechanism (CEM), intended to improve Union resilience to major threats and prepare for and mitigate the immediate impacts of large-scale incidents. Funding for the CEM is also to be derived from the Digital Europe Programme.[20] The CEM focuses on improving the resilience of entities operating in highly critical sectors (listed in Annex 1 and 2 of the NIS2

[11] Article 3(1), Cyber Solidarity Act Proposal.
[12] Article 3(2), Cyber Solidarity Act Proposal.
[13] Regulation (EU) 2021/694 establishing the Digital Europe Programme and Repealing Decision (EU) 2015/2240, available at EUR-Lex - 32021R0694 - EN - EUR-Lex (europa.eu).
[14] Article 4(1), Cyber Solidarity Act Proposal.
[15] Article 4(2) and Article 4(3), Cyber Solidarity Act Proposal.
[16] Article 5, Cyber Solidarity Act Proposal.
[17] Article 21(2), Cyber Solidarity Act Proposal.
[18] Articles 6 and 7, Cyber Solidarity Act Proposal.
[19] Article 8, Cyber Solidarity Act Proposal.
[20] Article 9, Cyber Solidarity Act Proposal.

Directive[21]) across the Union.[22] The CEM itself relies on three pillars - preparedness, response and recovery, and mutual assistance.[23]

Preparedness shall be fostered through coordinated testing exercises developed by the NIS Cooperation Group in cooperation with the Commission, ENISA and the High Representative, and will be employed with entities that operate in sectors identified by the Commission in consultation with the NIS Cooperation Group and ENISA, based on Annex 1 of the NIS2 Directive.[24]

Response and recovery shall be fostered through the European Cybersecurity Reserve, established to assist Member States, CSIRTs and Union entities by either responding or providing support in responding to large-scale incidents and recovering from them. This shall be done using incident responses services by trusted providers selected based on criteria listed in Article 16 of the Cyber Solidarity Act Proposal.[25] Member States, CSIRTs and Union entities may request support from the Reserve by providing information about the affected entity, potential incident impact, the planned use of the support, measure taken for incident mitigation, and other forms of support available.[26] These requests shall be assessed by the Commission with ENISA support and prioritized based on specified criteria. Member States, CSIRTs and Union entities must provide a summary report within a month of the support concluding.[27] In case of cybersecurity incidents leading to disasters or political crises, the CEMs services may be provided complementarily to appropriate crisis response mechanisms.[28] Finally, third countries may also request support from the Cybersecurity Reserve based on the conditions prescribed in Article 17.

Ex-Post Resilience – The Cybersecurity Incident Review Mechanism

Chapter 4 provides for a Union-wide incident review mechanism (Review Mechanism). The Commission, EU-CyCLONe or the CSIRT network may request a review of a specific incident from ENISA, pursuant to which ENISA must deliver an incident report.[29] The report shall be prepared in collaboration with entities relevant to the incident in question, including the affected entities when appropriate and other stakeholders (after they disclose any potential conflicts of interest) when required.[30] The report must cover causes, vulnerabilities and lessons, and must protect confidential information that may be part of its review.[31]

[21] Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), available at EUR-Lex - 32022L2555 - EN - EUR-Lex (europa.eu).
[22] Article 10(1), Cyber Solidarity Act Proposal.
[23] Article 10, Cyber Solidarity Act Proposal.
[24] Article 11, Cyber Solidarity Act Proposal.
[25] Article 12(1), Article 12(2) and Article 12(3), Cyber Solidarity Act Proposal.
[26] Article 13, Cyber Solidarity Act Proposal.
[27] Article 14, Cyber Solidarity Act Proposal.
[28] Article 15, Cyber Solidarity Act Proposal.
[29] Article 18(1), Cyber Solidarity Act Proposal.
[30] Article 18(2), Cyber Solidarity Act Proposal.
[31] Article 18(3), Cyber Solidarity Act Proposal.

3 Another piece in the cybersecurity puzzle

Overall, once finalised and adopted, the Cyber Solidarity Act will contain important measures for strengthening the EU's preparedness, management and responses to cybersecurity threats and incidents. With regard to next steps, the Court of Auditors and the Economic and Social Committee have adopted their opinions on the proposal.[32] The proposal is now at the Council of the European Union for the first reading after which it will proceed to the European Parliament.

The Cyber Solidarity Act proposal is the most recent addition to the EU's cybersecurity legal framework aimed at increasing the resilience of critical entities against cybersecurity risks and supporting the coordinated management of large-scale cybersecurity incidents and crises. The EU framework already in place consists of the NIS 2 Directive[33], the Cybersecurity Act[34], the Directive on attacks against information systems[35], and the Commission Recommendation on coordinated response to large-scale cybersecurity incidents and crises.[36] The Cyber Solidarity Act proposal builds on and bolsters the existing cybersecurity frameworks for operational cooperation and crisis management such as the EU-CyCLONe and the CSIRTs network. The cross-border SOCs are intended to complement the existing CSIRTs network by sharing, merging and analysing data on cybersecurity threats from both public and private entities.[37] Importantly, the Cyber Solidarity Act proposal will not affect the legal obligations of entities operating in critical and highly critical sectors laid down by the NIS 2 Directive.[38]

The Cyber Solidarity Act proposal also envisages close cooperation with the private sector. It aims to advance cross-border and public-private cooperation in anticipating and tackling cyber-attacks by pooling data from both public and private entities to deduce high quality intelligence on cybersecurity threats.[39] Furthermore, the EU Cybersecurity Reserve will consists of selected private providers of managed security services to support the response and immediate recovery in case of large-scale cybersecurity incidents.[40]

[32] Opinion of the European Economic and Social Committee on 'Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services' (COM(2023) 208 final) — 2023/0108 (COD) and on 'Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents' (COM(2023) 209 final]) — 2023/0109 (COD), EESC 2023/02408, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023AE2408.
Opinion 02/2023 of the European Court of Auditors concerning the proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, 2023/0109(COD) of 18 April 2023, available at https://www.eca.europa.eu/ECAPublications/OP-2023-02/OP-2023-02_EN.pdf.
[33] [33] Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), available at EUR-Lex - 32022L2555 - EN - EUR-Lex (europa.eu).
[34] 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 information and communications technology cybersecurity certification (Cybersecurity Act), available at https://eur-lex.europa.eu/eli/reg/2019/881/oj.
[35] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0040.
[36] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, available at https://eur-lex.europa.eu/eli/reco/2017/1584/oj.
[37] Section 1, Explanatory Memorandum for the proposed Cyber Solidarity Act, COM(2023) 209 final, Page 3.
[38] Section 2, Explanatory Memorandum for the proposed Cyber Solidarity Act, COM(2023) 209 final, Page 6.
[39] Recital 15, Cyber Solidarity Act proposal.
[40] Recital 33, Cyber Solidarity Act proposal.