European Parliament

Cyber solidarity act

OVERVIEW

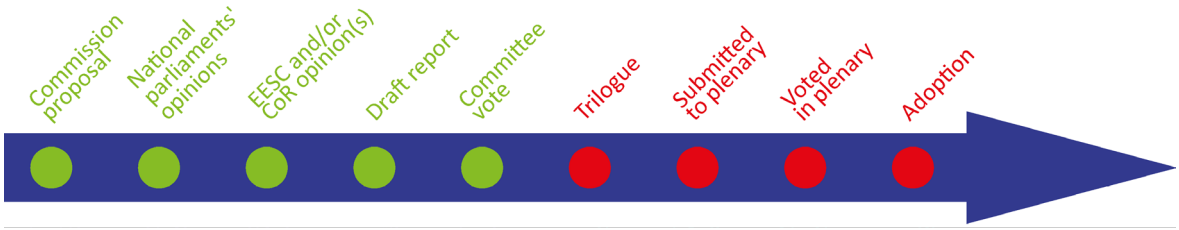
Russia's war against Ukraine has revealed the extent of our dependency on digital technology and the fragility of the digital space. It has triggered a surge in cyberattacks that have been particularly disruptive when targeting critical infrastructure – such as energy, health or finance – because of the increasing reliance on information technology, rendering this infrastructure all the more vulnerable.

Against this backdrop, the Commission has proposed a regulation on a cyber solidarity act that would address the urgent need to strengthen solidarity and EU capacities to detect, prepare for and respond to cybersecurity threats and incidents. The proposed regulation envisages the establishment of a framework based on three pillars. The first is a European cyber shield – a platform of national and cross-border security operations centres. The second is a cybersecurity emergency mechanism that would support – including financially – preparedness, response and mutual assistance actions among Member States by creating a European cybersecurity reserve of trusted providers. The third is a cybersecurity incident review mechanism to assess and review significant or large-scale incidents.

In Parliament, the file was assigned to the Committee on Industry, Research and Energy (ITRE), where Lina Gálvez Muñoz (S&D, Spain) was appointed rapporteur.

The Council and the Parliament are currently in negotiations to finalise the text.

Measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents		
Committee responsible:	Industry, Research and Energy (ITRE)	COM(2023)0209 18.4.2023
Rapporteur:	Lina Gálvez Muñoz (S&D, Spain)	2023/0109(COD)
Shadow rapporteurs:	Angelika Niebler (EPP, Germany) Bart Groothuis (Renew, Netherlands) Ville Niinistö (Greens/EFA, Finland))	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
Next steps expected:	Committee vote	



Author: Polona Car
Members' Research Service
PE 754.614 – February 2024

EN

Introduction

Digital technology, now ubiquitous, has had a positive impact on our societies. On the other hand, as we are more and more dependent on digital services and tools, it has made our societies more vulnerable as cyber incidents have surged. A 2023 ENISA report on the threat landscape in the EU revealed that cyber criminals spared no sector, with the public administration and healthcare being the two most frequently targeted. Ransomware tops the list of cyberattacks in the EU, closely followed by distributed denial of service (DDOS) attacks.[1] These attacks are becoming increasingly severe, complex and inexpensive to launch, and are increasingly targeting mobile networks and the internet of things (IoT).[2] Health service providers, pipelines, airports, ministries, hotel chains, banks, digital service providers are just a few of those who have suffered cyberattacks recently.[3] Russia is using information manipulation as one of its key weapons of aggression against Ukraine. Social engineering and information manipulation campaigns are misusing AI technologies for their attacks. Of particular concern are the growing capabilities of malicious entities, which are now attacking entire supply chains and increasingly using employees as entry points.

To efficiently detect and respond to these threats, societies need to ensure a fast and unimpeded exchange of information to shorten the detection time and mitigate the damage. According to the latest IBM report, the cost of data breaches globally has increased by 15.3 % since 2020, and the mean time to detect and contain breaches remains as high as 277 days or more than 9 months. This is especially relevant because as many as 22 % of EU enterprises experienced an ICT security-related incident in 2022, leading to unavailability, destruction or corruption of data, or disclosure of confidential data. Small and medium sized enterprises (SMEs) are particularly vulnerable, with those employing up to 50 employees accounting for 87 % of affected companies, according to a recent analysis.

Russia's hybrid approach, merging physical and cyberattacks, has demonstrated that disruption of essential services poses a realistic threat to the EU. For example, the attack on the KA-SAT satellite communication provider just 1 hour before Russia's attack on Ukraine affected internet services and wind farms across Europe. Healthcare – one of the critical sectors– is among the most frequently attacked. According to a 2023 ENISA report, 80 % of health organisations surveyed reported that more than 61 % of their security incidents had been caused by vulnerabilities. Cyberattacks are increasingly used in modern warfare.

As borders are not an issue for malicious entities posing cybersecurity challenges, efforts are made to address them collectively. ENISA's 2022 Cyber Europe exercises identified vulnerabilities in the cybersecurity posture of the private and public stakeholders involved in the exercises. Similarly, they identified how EU-wide coordination could improve when major cyber incidents occur[4] and revealed the need for cooperation and information exchange. This is even more important in view of the fact that 77 % of EU citizens underline the need for greater cybersecurity and safety of digital technologies to facilitate their daily use. Moreover, respondents to the 2023 Eurobarometer survey list the protection of users from cyberattacks as the EU citizens' top priority for future actions in their countries.

Existing situation

The European cybersecurity strategy of 2020 announced the creation of a European cyber shield. The shield would reinforce cyber threat detection by building a network of security operations centres (SOCs)[5] across the EU as well as developing high-quality threat intelligence underpinned by latest artificial intelligence (AI). Improving resilience to cyberattacks is one of the general objectives of the digital decade policy programme 2030, defined in the Decision of the European Parliament and of the Council establishing the Digital Decade Policy Programme 2030.

In line with the priority highlighted in Commission President Ursula von der Leyen's 2021 State of the Union Speech, in November 2022 the Commission presented the EU policy on cyber defence,

aimed at increasing the EU cyber defence capabilities and synergies between military and civilian cyber communities. As part of the policy, the Commission committed to launching an EU cyber solidarity initiative to strengthen common EU detection of cyber threats and incidents as well as preparedness and response capabilities. This commitment started taking shape just a few weeks later in the form of a call for expression of interest, coordinated with the European Cybersecurity Competence Centre (ECCC), for selecting hosting entities for cross-border cyber threat detection platforms. That was the first phase of deployment of the European infrastructure of cross-border SOCs.

A substantial legislative framework for countering cybersecurity threats and for supporting a coordinated response to large-scale incidents is already in place. The urgency to step up the efforts to detect and mitigate cyber threats has however increased dramatically since Russia's attack on Ukraine.

The proposed cyber solidarity act (CSoA) would complement and build on structures established in accordance with legislation that has already been adopted and programmes that are already running. Some of these structures, pieces of legislation and programmes are described below.

- Directive on Security of Network and Information Systems across the EU (the NIS Directive) was the first horizontal legal act aimed at improving the cybersecurity in the EU by setting measures, notably to protect critical infrastructure. Due to a changing threat landscape, the Directive on the security of network and information system (NIS2) will replace the NIS Directive and needs to be transposed into national law by October 2024. NIS2 broadens the scope of application of the directive by adding new sectors and addressing the issues related to the transposition and implementation of its predecessor. NIS2 introduces the European Cyber Crises Liaison Organisation Network (EU-CyCLONe), a rapid crisis management coordination system to be activated during large-scale cross-border cyber incidents.
- The Cybersecurity Act strengthened the role and powers of ENISA. It furthermore introduced a voluntary certification scheme to ensure compliance with the mandatory safety requirements laid out in legal acts seeking to safeguard the integrity of the certification schemes in the internal market.
- The Directive on attacks against information systems harmonised criminalisation and sanctions for offences aimed against information systems.
- The Commission recommendation on coordinated response to large-scale cybersecurity incidents and crises set out a 'blueprint' for a coordinated approach to crisis cooperation across the various elements of the cyber ecosystem to foster utilisation of the NIS Directive.
- The European Cybersecurity Competence Centre (ECCC) is responsible for EU cybersecurity capacity building. The centre aims to improve technological sovereignty through strategic cybersecurity investments. Together with the Network of National Coordination Centres (NCCs), it forms the cybersecurity shield for the EU powered by AI. It became operational in May 2023.
- The Joint Cyber Unit (JCU) platform, which should have been fully implemented by 30 June 2023, would assure a coordinated response between civilian, law enforcement, diplomatic and cyber defence communities.
- The Integrated Political Crisis Response Mechanism (IPCR) provides necessary protocols and procedures for rapid and coordinated decision-making by the EU during major and complex crises.
- The Union Civil Protection Mechanism (UCPM) gives the EU additional capacities to respond to new risks.
- The EU cyber diplomacy toolbox can address external-action responses to large-scale incidents.
- The Digital Europe Programme (DEP) Regulation aims to support the digitalisation of Europe and the digital single market, and to help the EU and its Member States achieve digital sovereignty. The DEP envelope of €7.6 billion includes €1.6 billion for cybersecurity (DEP specific objective 3).

Parliament's starting position

In its resolution on cyber defence of June 2018, the European Parliament called for a coherent development of cyber capacities across all EU institutions and bodies as well as across the Member States. The Parliament also called for providing political and practical solutions to help overcome the remaining political, legislative and organisational obstacles to cooperation on cyber defence.

Similarly, in its resolution on the state of EU cyber defence capabilities of October 2021, Parliament called for further integration of cybersecurity into EU crisis response mechanisms. Specifically, it suggested linking the existing initiatives, structures and procedures across various cyber communities with a view to ensuring enhanced mutual assistance and operational cooperation between Member States in the event of major cyberattacks.

Council starting position

In its conclusions on the development of the EU's cyber posture of May 2022, the Council called on the Commission to create an emergency response fund for cybersecurity that would fully prepare the EU and its Member States to face large-scale cyber incidents. In its conclusions on ICT supply chain security, Council insisted on the need to enhance EU competitiveness in the area of cybersecurity by securing funding for programmes such as the Horizon Europe programme for research and innovation and the DEP; doing so would help reinforce the capacities of the EU digital economy, society and democracy. In December 2022, the Council adopted the Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure, with a view to stepping up the efforts to protect critical infrastructure and to foster inter- and intra-EU cooperation.

Preparation of the proposal

The proposed regulation for a cyber solidarity act was not accompanied by an impact assessment due to the urgency involved. The Commission states that actions envisaged by the proposal are in accordance with the DEP Regulation, for which a dedicated impact assessment was carried out. Furthermore, the Commission states that the proposal follows on from a call by the Council to set up an emergency response fund for cybersecurity. This resulted in a call for expression of interest for the joint procurement of tools and infrastructure to establish cross-border SOCs, and a call for grants to enable the capacity building of SOCs serving public and private organisations. Moreover, the Commission set up a short-term programme to support Member States in the implementation of the DEP. This short-term programme, which is being implemented by ENISA, includes preparedness and incidence response actions, such as penetration testing of critical entities, and will continue until the proposed regulation becomes adopted and enters into force. The programme will thus assure funding for cyber detection projects also beyond 2027. The programme facilitated the preparation of the regulation.

The changes the proposal would bring

The Commission presented on 18 April 2023 a proposal for a regulation laying down measures to strengthen solidarity and capacities in the Union to **detect**, **prepare for** and **respond** to cybersecurity threats and incidents.

The proposal addresses in particular the urgent need to strengthen collective detection and situational awareness of cyber threats and incidents in critical and highly critical sectors as well as developing EU-wide response capacities to respond to large-scale incidents. The aim is to **increase EU resilience** through the exchange of information and cooperation among Member States to enable them to respond to surging cyber threats and to **ensure funding** for tackling cyberattacks.

The legal basis is Article 173 of the Treaty on the Functioning of the European Union, which ensures the conditions necessary for maintaining the competitiveness of the EU industry. In this respect, the

proposal aims to increase in particular the resilience of critical and highly critical sectors. The proposal is also based on Article 322(1), point (a) TFEU, which contains specific carry-over rules derogating from the principle of annuity set out in the Financial Regulation, and thereby allowing for a certain degree of flexibility in the financial management of the cybersecurity emergency mechanism.

The proposal aims to meet its objectives through:

- the deployment of a European cyber shield,
- the creation of a cyber emergency mechanism, and
- the establishment of a cybersecurity incident review mechanism.

European cyber shield[6]

The European cyber shield will be an interconnected pan-European **platform of public national and cross-border SOCs**.[7] Its aim will be to **improve the detection, analysis and response** to cyber threats and as such the development of the cyber community through the **gathering and sharing of data, and the production of cyber intelligence**. The European cyber shield will cooperate with the pan-European High Performance Computing infrastructure on development of AI and data analytics. It will **use state-of-the-art technology** for advanced data collection and analytics tools, to contribute to enhancing cyber detection and management capabilities and providing real-time situational awareness. The **ECCC will implement the actions** related to the European cyber shield.

Each Member State will designate **at least one national SOC** to act as **a reference point** for collecting and analysing information on cybersecurity threats and incidents and will contribute to the work of cross-border SOCs. A **hosting consortium** of national **SOCs from at least three Member States** will be eligible to establish a **cross-border SOC**.

Requirements towards the joint procurement of tools and infrastructure with the ECCC:

- The ECCC selects the national SOC/hosting consortium to participate in the joint procurement.
- The grants awarded are allocated as follows: up to 50 % for national SOCs and 75 % for hosting consortia to cover the acquisition costs of the tools and infrastructure. Up to 50 % of the grants cover operation costs.
- Member States/hosting consortium cover the remaining costs.
- Hosting and usage agreements regulate the usage of the tools and infrastructure between the ECCC and the national SOC/hosting consortium.
- A national SOC would need to participate in cross-border SOCs within 2 years after receiving EU funding, after it has been selected to participate in a joint procurement.

Participants in a hosting consortium that has established a cross-border SOC will **share cyber threat information** with each other, based on a written consortium agreement, but also with other cross-border SOCs, based on cooperation agreements, and with other relevant EU entities. **Interoperability** between cross-border SOCs should be assured (as regards data formats, taxonomy, data handling and data analysis tools, and secure communications channels) and can be specified by the Commission with an implementing act.

When information concerns a **potential large-scale threat**, the cross-border SOC will **share information with EU CyCLONe, the computer security incident response teams (CSIRTs) network and the Commission**, in accordance with the NIS2 Directive. Information will be shared on a need-to-know principle and will comprise technical information, information about the nature and motives of the attacker or potential attacker, and higher-level non-technical information about a potential or ongoing large-scale cybersecurity incident.

The European cyber shield will complement and support entities and networks responsible for crisis management in the EU, notably the EU-CyCLONe. It will gradually develop dedicated protocols and standards to allow for cooperation with the cyber defence community.

Funding of the shield will be implemented in accordance with the DEP Regulation.

Cybersecurity emergency mechanism

The cybersecurity emergency mechanism is the second pillar of the proposed regulation, intended to increase the EU's preparedness and response capacity in case of major incidents, by enabling the provision of cybersecurity assistance. The mechanism will support three types of actions: **preparedness**, **response** and financial support for **mutual assistance** between Member States. It will improve the preparedness and response to cybersecurity incidents by **testing preparedness in critical sectors** for potential vulnerabilities. The list of entities operating in highly critical sectors, included in the coordinated preparedness testing, will be regularly reviewed by the Commission and ENISA, according to the NIS2 Directive.

The mechanism will create an **EU cybersecurity reserve**, ready to intervene in case of significant or large-scale cybersecurity incidents affecting the Member States. It will be **composed of incident response services from trusted providers**[8] certified in accordance with the EU certification scheme for managed security services, once the scheme becomes available. The services making up the reserve will **support Member States** in providing assistance to entities in critical and highly critical sectors. This assistance will be complementary to the support already being provided at national level, without prejudice to the NIS2. Its users will include Member States' cyber crisis management authorities and CSIRTs and EU institutions, bodies and agencies. The Commission will bear overall responsibility for the implementation of the reserve, which it could entrust in part or in full to ENISA.

ENISA will prepare a mapping of the services needed for the establishment of the reserve. Users should take mitigating measures of their own to receive support from the reserve. **Requests for support** should be transmitted to the Commission and ENISA via the **single point of contact**. **Third countries** will also be able to request support from the reserve, providing they have concluded association agreements[9] for participation in the DEP. Such requests will be coordinated with the EU High Representative.

The actions undertaken as part of the cybersecurity emergency mechanism should be coordinated with the cyber diplomacy toolbox where appropriate.

Funding will be provided under the DEP Regulation.

Cybersecurity incident review mechanism

The aim of the mechanism will be to **assess and review significant or large-scale incidents**. **ENISA** should review such incidents at the request of the Commission or national authorities (EU-CyCLONe or the CSIRTs network), report in the form of an **incident review report** on lessons learned and give recommendations to improve the EU's cyber posture, when appropriate. To prepare the report, ENISA would collaborate with all relevant stakeholders. When an incident relates to a third country, the Commission should share the report with the EU High Representative.

Amendments to the DEP Regulation and reporting obligation

Amendments to the DEP Regulation are necessary to enable the **establishment of the cyber shield** as well as the establishment and operation of the **cyber emergency mechanism**, including the creation of the cyber reserve. In addition, such amendments would need to clarify the conditions for eligibility for financial support and the conditions under which **unused commitments** could be **carried over**,[10] given the unpredictable, exceptional and specific nature of the cybersecurity landscape.

The Commission will have to publish **regular reports** as a basis for the evaluation of the regulation by the Council and the Parliament. The first report will be due 4 years after the date on which the regulation becomes applicable.

Under the CSoA, the Commission will be empowered to issue implementing acts.

Advisory committees

The European Economic and Social Committee (EESC) adopted its opinion on the CSoA on 13 July 2023. In this document, the EESC asks that more attention be paid to the principles of proportionality and subsidiarity in the cybersecurity field, and objects to the proposed implementing powers,[11] since cybersecurity is a responsibility of the Member States. The EESC underlines the importance of procuring exclusively EU technology to equip national SOCs. Furthermore, the EESC expresses a concern about the absence of cybersecurity certification schemes 4 years after the adoption of the EU Cybersecurity Act and proposes the involvement of sectoral agencies in their future development. The EESC underlines that the response to an incident should also include hardware and software, not only capabilities and processes. It believes that ENISA should receive adequate funding and resources in view of its strengthened role.

The EESC proposes that the SOCs participating in a consortium should hold a coordinating leadership role on a one-year rotation basis and that the hosting consortium should receive 100 % of EU funding for the tools and infrastructure, as opposed to 75 % as proposed by the Commission. The EESC finds that the cost estimates of the proposal are inadequate. The same applies to the envisaged EU-level funding, to which private resources should be added. The EESC finds that the procedure involved in requesting support from the EU cybersecurity reserve lacks clear deadlines for the response that needs to be given. It is disappointed by the lack of involvement of the social partners and civil society in the drafting of the regulation. The EESC welcomes the European cybersecurity academy initiative and underlines the need to establish indicators that measure progress on reducing cybersecurity skills gaps. It also proposes that the planned evaluation of the regulation after it enters into application should take place 2 years as opposed to 4 years, as proposed by the Commission, and it should be accompanied by an impact assessment.

The Committee of the Regions (CoR) adopted an opinion on the EU Cyber Solidarity Act and Digital Resilience on 30 November 2023. In its opinion, the CoR welcomes the specific objectives of the draft regulation and the measures proposed therein. It finds it regrettable, however, that, despite increasing cyber attacks, local and regional authorities are not sufficiently covered by the current proposal, and therefore proposes a number of legislative changes to address these shortcomings. In particular, the CoR requests that – in order to avoid a situation where local authorities responsible for essential operations in some Member States fall outside the scope of the CSoA – it be made clear in the legal text that such authorities are considered to be included whether or not they are covered by the NIS 2 Directive.

The CoR therefore considers it important for the regulation to aim to reduce differences in the field of cybersecurity maturity, also within countries, and to ensure that all involved players have relatively equal abilities and ambition. In addition, the CoR urges the Member States, the Commission and all local authorities to join together in raising awareness of the need for action, including the need to increase investment in digital resilience, particularly at local and regional level, and to consider developing protective policy instruments targeting financial ransomware attacks. This will require appropriate financial, technical and upskilling efforts.[12] Finally, the CoR recommends that, within the framework of the European Cyber Shield, indicators should be developed to determine how development and maturity are increasing in connection with the introduction of the regulation. In the long term, the indicators can feed into a data-based risk map, demonstrating where the greatest need for action is.

National parliaments

The deadline for subsidiarity scrutiny was 27 July 2023. No reasoned opinions were sent to the Parliament by the deadline. The Czech Senate and Chamber of Deputies, the French Senate and the Portuguese Assembly of the Republic adopted political dialogue resolutions on the proposed CSoA.

Stakeholder views[13]

The proposal was not preceded by a public consultation due to its pressing nature. Its publication drew a weak stakeholder response, which came mainly from the private sector.

As described above, the Commission refers to the consultation conducted for the Digital Europe programme. Furthermore, the Commission states that the initial actions[14] that facilitated the drafting of the proposal were undertaken in close cooperation with stakeholders. The Commission organised a workshop on the cyber emergency mechanism with Member State experts on 16 February 2023.

European Court of Auditors highlights the risks

The European Court of Auditors (ECA) published a mandatory opinion on the proposal following requests from both the Parliament and the Council. The ECA underlined that national security, including responding to cybersecurity incidents, is a responsibility of the Member States. That does not however exclude common actions in case of large-scale incidents. The ECA thus welcomed the proposal but underlined that it could create more complexity in the EU cybersecurity 'galaxy',[15] in particular considering the overlap between the existing CSIRTs network and the SOCs. In the ECA's view, this risk could be mitigated by consolidating the structures and clarifying how they should interact.

The ECA further underlined the absence of an impact assessment and the fact that information on funding and resources is only partial. To address the latter, the ECA suggested publishing cost estimates to increase transparency. The ECA questioned the decision of the lawmaker to assign different rates for the financing of tools and infrastructure (50 % for national and 75 % for cross-national SOCs). It also pointed to the lack of information on the period for which EU co-financing of operating costs should be extended, arguing that it involves the risk of creating dependency on EU financing. The ECA furthermore considered that the lack of reporting requirements could hinder the work in terms of collection and analysis of information for national SOCs.

The ECA highlighted the risk that a potential lack of effective information sharing might undermine the EU cybersecurity shield. In this respect, it welcomed the proposal's specific provisions for actions to mitigate this risk in Articles 4, 5 and 6,[16] and stressed the importance of ensuring that cross-border SOCs share information with the EU-CyCLONe, CSIRTs network and the Commission in case of large-scale incidents. The ECA was critical of the lack of a pre-defined deadline for a request for support from the cybersecurity reserve and a response from the Commission.

As far as the derogation from the principle of annuality is concerned, the ECA considered that it could be justified only for support funds used from the cybersecurity reserve but not for the preparedness actions. In addition, a carry-over of unused commitments should be limited to the following year, but not beyond it. The ECA also proposed a maximum deadline for ENISA to deliver an incident review report after an incident and insisted that the proposal should specify how ENISA's recommendations should be followed up. The ECA considered that the 4 year-period envisaged for the evaluation of the regulation should be advanced.

Relation with the private sector

Digital Europe (trade association representing digitally transforming industries in Europe) published an opinion that recommends strengthening cooperation and information sharing between SOCs and information sharing and analysis centres (ISACs), tasked with fostering the sharing of

information on threats and vulnerabilities in the private sector. The paper points to the need of including the private sector among other things in the establishment of the European cyber reserve. Digital Europe is critical towards procurement procedures, arguing that they should be sped up and simplified in collaboration with the private sector.

AmCham EU (American Chamber of Commerce to the European Union) underlines the need for the SOCs within its scope to cooperate with the entities covered by the NIS2 Directive. Furthermore, it proposes establishing an EU Cyber Solidarity Group. This group – composed of representatives of ENISA, the CSIRT Network, the chair of the NIS Cooperation Group and the trusted providers – should serve as a platform for regular consultations between public and private partners on the implementation and deployment of the cross-border SOCs and the cyber reserve.

Covington (a law firm specialised in data privacy and cybersecurity) experts underline that the CSoA does not oblige private entities to share their cyber intelligence with the SOCs. On the other hand, the NIS2 Directive obliges Member States to promote voluntary information sharing, and it is not yet clear how the CSoA will meet this obligation.

International dimension

Digital Europe considers that collective defence could be enhanced by inclusion of professionals from NATO-allied countries, EU-candidate- and like-minded countries (e.g. Switzerland and Israel). Moreover, it suggests that cross-border SOCs operations should be based on cloud technology.

AmCham EU proposes creating partnerships with global providers to strengthen prevention and mitigation capabilities based on global datasets and to enable a cross-border and cross-sectoral perspective. Moreover, AmCham EU opposes the inclusion of politically sensitive concepts such as technological sovereignty in the proposal, because it ignores the global nature of cyberattacks and undermines the ability to fight them. In their view, global providers could contribute to building information-sharing platforms between strategic partners. To this end, they propose amendments to clarify the role of private SOCs in cross-border SOCs.

Similarly, SecurityScorecard (an information security company) emphasises the international dimension of the cyber shield and the need for cooperation with international partners (the United States, NATO and other like-minded countries) because of the rising global nature of cyber threats. The European cyber shield should focus on real-time data and cyber risk ratings. Cooperation would encourage the development of international cybersecurity standards.

Forrester (research and advisory company) analysts highlight the fact that the proposal does not consider third-party risk and the need for actions aimed at strengthening the cybersecurity of emerging economies. National cybersecurity should be a priority for countries joining the EU. Moreover, they express a concern that the regional imbalance in data sharing could hinder cross-border collaboration.

Trusted providers

Cisco (IT and networks multinational company) welcomes the creation of a pool of trusted providers but warns about the potential limiting effect of language requirements and future certification of services. Their study reveals that keeping a reserve of internal staff for incidence response as well as having external incident response services has a positive effect (15 % higher resilience scores on average), and that a combination of both has an even bigger positive effect on security resilience.

Covington experts underline that the criteria for the selection of trusted providers do not exclude the possibility for non-EU providers to be part of the European cybersecurity reserve. In this respect, they raise concerns about sovereignty demands in proposed cloud services certification, as this could be reflected in the certification of security providers as well. Similarly, AmCham EU advocates participation by trusted providers in information-sharing and capacity-building arrangements with the EU, and proposes to allow non-EU providers to participate in initiatives under the Act, such as the EU cybersecurity reserve.

Legislative process

In the Parliament, the file was assigned to the Committee on Industry, Research and Energy (ITRE), and Lina Gálvez Muñoz (S&D, Spain) was appointed as rapporteur. The Committees on Foreign Affairs (AFET), Transport and Tourism (TRAN), Budgets (BUDG), Internal Market and Consumer Protection (IMCO), Civil Liberties, Justice and Home Affairs (LIBE), and on Budgetary control (CONT) were asked to deliver opinions. All except the first two decided not to give an opinion. The AFET committee published an opinion on 27 October 2023 and the TRAN committee published its opinion on 25 October 2023.

The ITRE committee adopted its report on 7 December 2023 by 43 votes to 10, with one abstention. The committee's decision to enter into negotiations with the Council was confirmed by Parliament as a whole during the December plenary.

The ITRE committee report, inter alia:

- adds, to the objectives of the regulation, support for industrial capacity in the cybersecurity sector, particularly for microenterprises and SMEs, including start-ups, to contribute to **open strategic autonomy** and **technological sovereignty**, competitiveness, and resilience in the sector and ensure strong Union capabilities, also in cooperation with international partners. To the specific objectives, it adds **development of skills** and competencies of the workforce;
- adds clarity to the text by **expanding certain definitions**. For example, it includes a definition for a National Security Operations Centre or National SOC;
- requests that **National SOCs** should be **incorporated into the CSIRTs** or other existing cybersecurity infrastructures and governance, when possible;
- excludes entities established in countries that are not part of the Agreement on Government Procurement from participation in joint procurement on tools and infrastructures with a Hosting Consortium;
- promotes the **exchange of cyber threat intelligence** between National and Cross-border SOCs and industry ISACs with the aim of preventing, detecting, or mitigating threats;
- requests that the Commission assess the working of the cybersecurity emergency mechanism annually;
- introduces a certain flexibility to the provision of services through the EU cybersecurity reserve by allowing **conversion of unused procured incident response services from trusted providers into exercises or training** for dealing with incidents;
- empowers the Commission to adopt **delegated acts** (which give Parliament the right of scrutiny) to supplement the regulation, rather than giving the Commission the prerogative of adopting implementing acts (which are adopted in a procedure where Parliament has no powers);
- limits the amount for the establishment and implementation of the EU Cybersecurity Reserve to €27 million to reduce the impact of the reduction of funding on other DEP priorities;
- requests **more resources for ENISA** to carry out additional tasks, without jeopardising other Union programmes, particularly the DEP;
- details the **evaluation and review process** for the regulation, which should take place every two years.

The Council adopted the negotiating mandate at the Coreper meeting on 20 December 2023. The Council clarified the terminology and adapted it to the requests of Member States (in particular on SOCs, which are renamed 'Cyber Hubs', and the Cyber Shield, which is renamed the 'Cybersecurity Alert System'). The Council also revised the definitions, to bring them into line with the NIS2 Directive.

The Council clarified the interaction between the entities defined in the proposal and the existing structures, underlining that actions under the regulation will be complementary to the activities carried out by the CSIRTs network, the NIS Cooperation Group, and EU-CyCLONe. In particular, the Council stressed the voluntary nature of Member States' involvement throughout the text, stressing that national security remains the responsibility of the Member States. The Council also stressed the importance of confidentiality in the exchange of information for all three pillars. This should be limited to what is relevant and be proportionate to the purpose of the exchange, in order to preserve the confidentiality and protect the security and commercial interest of those involved. It would exclude exchanges of information that could be contrary to the Member States' essential interests in terms of national security, public security or defence if disclosed.

Interinstitutional negotiations on the proposal started on 13 February 2024.

EUROPEAN PARLIAMENT SUPPORTING ANALYSIS

Negreiro M., Managed security services, Briefing, EPRS, October 2023.

Negreiro M., The NIS2 Directive, A high common level of cybersecurity in the EU, Briefing, EPRS, February 2023.

Negreiro M. ENISA and a new cybersecurity act, Briefing, EPRS, 2019.

Negreiro M. with Belluomini A., The new European cybersecurity competence centre and network, Briefing, EPRS, European Parliament, 2020.

Szczepanski M., Digital Europe programme Funding digital transformation beyond 2020, Briefing, EPRS, May 2021.

OTHER SOURCES

Measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, Legislative Observatory (OEIL).

ENDNOTES

1 A Cisco report estimates that the DDoS attacks will double from 7.9 million in 2018 to 15.4 million by 2023 globally.

2 Internet of Things (IoT) devices and networks are increasingly suffering from DDoS attacks as their resources are often limited, which causes poor security features. Weak passwords, for example, make devices easy to corrupt. This trend was also highlighted in the Microsoft Digital Defense Report 2022.

3 For details on incidents, see B ANNEX: INDICATIVE LIST OF INCIDENTS in the ENISA Threat Landscape 2022 report.

4 Cyber crisis management was also tested in the framework of the Blue OLEx exercise, which tested the standard operating procedures of the European cyber crisis liaison organisation network (EU-CyCLONe) applied when network members contribute to operational coordination in case of large-scale cyber incidents.

5 SOCs are teams (private or public) that detect and then act on cyber threats. They work with computer security incident response teams (CSIRTs), which handle computer security. CSIRTs often also have other responsibilities and typically play a horizontal role in organisations. In bigger entities, SOCs usually contribute to the work of CSIRTs with their monitoring and detection capabilities, while CSIRTs handle incidents. In smaller entities, the two teams can be identical.

6 The setting up of the European cyber shield has already started. The first phase was initiated by a call for expression of Interest to establish a cross-border infrastructure of European security operations centres (SOC) under the DEP cybersecurity work programme 2021-2022.

7 The European cyber shield has national SOCs (public bodies designated by Member States to fill this role at national level) as well as cross-border SOCs consisting of at least three national SOCs. The proposal gives a definition of a 'Cross-border Security Operations Centre' (Article 2(1)), but no definition of Security Operation Centres (SOCs).

8 These are managed security service providers as defined in Article 6, point (40) of the NIS2 Directive.

9 See the heading 'Who is eligible to participate in the Digital Europe Programme'. Since this publication, four new agreements have been signed: with Montenegro, North Macedonia, Albania, and Serbia.

10 Article 19 (2)(b) specifies that carry over is automatic and may be committed and paid up to 31 December of the following financial year.

11 They are listed in recital (38) of the proposal

12 The impact of ransomware on local and regional authorities was discussed in detail in a study commissioned by the Committee of the Regions in 2023.

[13] This section aims to provide a flavour of the debate and is not intended to be an exhaustive account of all different views on the proposal. Additional information can be found in related publications listed under 'European Parliament supporting analysis'.

[14] As already described, these actions included development of cross-border SOCs platforms, with a call for expression of interest, and a short-term programme to assist the Member States through DEP funding allocated to ENISA.

[15] See the Annex (p. 14) to the opinion on The European cybersecurity galaxy.

[16] The ECA provided the following examples: funding should be made available to national SOCs only if they commit to participating in cross-border SOCs, and members of cross-border SOCs should be required to share a 'significant amount of data' with each other. The ECA highlights that the support received during the first 2 years if a national SOC does not join a cross-border SOC does not need to be reimbursed.

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)

Second edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.