RÉPUBLIQUE FRANÇAISE

SÉNAT

EUROPEAN AFFAIRS COMMITTEE

Paris, 13 December 2023

POLITICAL OPINION

Political opinion relating to the 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 COM(2023) 209 final

The Senate European Affairs Committee,

Having regard to the Treaty on European Union, in particular Article 4,

Having regard to the Treaty on the Functioning of the European Union, in particular Articles 173 and 322,

Having regard to Regulation (EU) 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers,

Having regard to 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 and repealing Regulation (EU) No 526/2013 (Cybersecurity Act),

Having regard to 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,

Having regard to Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres,

Having regard to 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),

Having regard to the Proposal for a Regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union COM(2022) 122 final,

Having regard to the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454 final,

Having regard to the Proposal for a Regulation pertaining to an extension of the scope of European cybersecurity certification, COM(2023) 208 final,

Having regard to the Proposal for a Regulation whose aim is to improve European solidarity in cybersecurity, COM(2023) 209 final,

Having regard to the Communication of 18 April 2023 announcing the creation of the European Cybersecurity Skills Academy, COM(2023) 207 final,

Having regard to Opinion 02/2023 of 5 October 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,

Having regard to the Senate's European Resolution 109 (2017-2018) of 26 May 2018 on the Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM(2017) 477 final,

Having regard to information report 458 (2017-2018) by Senators René DANESI and Laurence HARRIBEY on behalf of the Senate European Affairs Committee, entitled "*La cybersécurité : un pilier robuste pour l'Europe numérique*",

Having regard to Senator Laurence HARRIBEY's remarks of 5 July 2023 before the Senate European Affairs Committee on the compliance with the principle of subsidiarity of the European 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 COM(2023) 209 final,

On the Proposal for a Regulation and its objectives

Whereas cybersecurity is a major political issue given the widespread use of digital technology in our contemporary societies;

Whereas one of the consequences of the widespread digitalisation of European societies and economies is the European Union and Member States' growing vulnerability to cyberattacks;

Whereas, according to ENISA, the cybersecurity threat facing the European Union is now substantial and has increased since the start of the war in Ukraine;

Whereas for France, according to ANSSI (*Agence nationale de la sécurité des systèmes d'information*), cyberattacks affect public administrations, healthcare institutions and small and medium businesses whilst undermining our citizens' daily activities,

Whereas these threats and attacks are not just the acts of "hackers" and criminal networks but of state actors who are hostile to Member States and want to weaken the European Union;

Whereas, consequently, cooperation and mutual aid in cybersecurity between Member States is necessary and a prerequisite to a safe digital space;

Welcomes the fact that the European Union has recognised this need and established a solid, comprehensive legal framework to build a European cybersecurity architecture;

Recalls that this architecture was established by Regulation (EU) 2019/881 of 17 April 2019, which reinforced ENISA, and Directive (EU) 2022/2555 of 14 December 2022, known as NIS 2, which both imposed cybersecurity obligations on essential entities and created operational bodies to cooperate and exchange information;

Notes the European Commission's desire to further strengthen this architecture with this Proposal for a Regulation; questions the wisdom of presenting a new European text modifying cybersecurity players' relations and missions only four months after the final adoption of the NIS 2 Directive; nevertheless supports its objective in that it expresses a desire for increased and lasting cooperation on cybersecurity at the European level;

On the lack of an impact assessment accompanying the Proposal and its consequences for the assessment of the need for reform

Regrets the lack of an impact assessment accompanying the Proposal for a Regulation as this undermines the sincerity of the European Commission's presentation, prevents an estimate of the funding needed to implement the reform and makes it difficult to assess the proposed system's added value;

On the proposed regulation's scope of application

Whereas the wording of Articles 1 and 2 of the Proposal for a Regulation is ambiguous in that it does not explicitly exclude the fields of national security and national defence from its scope;

Whereas, moreover, the aforementioned Article 1(3) refers to a "primary responsibility" that is not exclusive of the Member States in the field of national security;

Recalls that, in accordance with the Treaties and in particular Article 4 of the Treaty on European Union (TEU), which stipulates that "national security remains the sole responsibility of each Member State", national security and national defence remain the exclusive competence of the Member States; considers that there can be no question of including the Member States in a mechanism for the massive and compulsory exchange of information with a large number of partners, which, paradoxically, would weaken the European Union's cybersecurity;

Invites the European Commission to ensure that the provisions of this proposal are compatible with those of the NIS 2 Directive; requests that paragraphs 6 and 7 of the aforementioned NIS 2 Directive be explicitly included in Article 1 of the proposal to specify that its provisions would be "without prejudice to the Member States' responsibility for safeguarding national security and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order", and that it would not apply "to public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement";

On the funding for the Proposal for a Regulation

Whereas the budget for cybersecurity actions under the Digital Europe programme has been increased by €100 million through a reallocation of funds, from €743 million to €843 million;

Notes, as confirmed in Opinion 02/2023 from the European Court of Auditors, that the information on this reform's financing is incomplete and, in particular, that the Proposal does not contain an estimate of the total expected cost of establishing and implementing the proposed measures; calls, therefore, on the European Commission to make these costs fully transparent;

Notes also that the European Commission wishes to be able to depart from the principle of annual budgeting in using the European funds earmarked for this mechanism; urges the European

Commission to limit this departure only to activities that cannot be planned, namely the European cybersecurity reserve and mutual assistance, since the latter would be implemented only to deal with unforeseeable events;

Recalls the need for sustainable national and European funding to guarantee the effectiveness of European cybersecurity cooperation;

Regrets that the redirection of funds to finance the present initiative is to the detriment of other essential initiatives such as digital education and the Erasmus+ programme, which aim to enhance our fellow citizens' digital skills and prevent "digital exclusion";

On the creation of a European "cybershield"

Whereas the threats to cybersecurity cannot, by their very nature, be completely countered, and there is no such thing as "zero risk" in cybersecurity;

Whereas the current European architecture resulting from the aforementioned NIS 2 Directive already includes multiple players responsible for policy coordination, such as the European cooperation group on cyber crisis management and prevention, such as the EU-CyCLONe network, and incident response, such as the computer security incident response teams (CSIRT);

Whereas this Proposal provides for the creation of a European "cybershield", a pan-European infrastructure consisting of national and cross-border security operations centres (SOCs), which should provide the European Union with advanced capabilities for detecting, analysing and processing data related to cybersecurity threats;

Whereas each Member State should set up a public body known as a national SOC, which would act as both a "radar" for the early detection of cybersecurity incidents and a point of reference for other, public and private organisations at the national level;

Whereas these national SOCs could acquire cybersecurity tools and infrastructures jointly with the European Cybersecurity Competence Centre (ECCC), receiving European financial aid

covering up to 50% of the acquisition costs and 50% of the operating costs;

Whereas at least three Member States, represented by their national SOCs, could come together within a host consortium to form a cross-border SOC;

Whereas these cross-border SOCs, in the case of a joint acquisition with the ECCC, could receive financial aid of 75% of the tool and infrastructure acquisition costs and 50% of operating costs;

Whereas these cross-border SOCs would be required to exchange relevant information, including on vulnerabilities, avoided incidents, and cybersecurity threats, not only among themselves but also, "without undue delay", with the CSIRT network, the EU-CyCLONe network and the European Commission, in the event of information relating to a major cybersecurity incident;

Whereas if a national SOC fails to join a cross-border SOC within two years, it will lose the benefit of any European aid;

Approves the European Commission's desire to improve the detection of cybersecurity incidents and threats at the European level;

Considers that the term "cybershield" is misleading and should be replaced by the more accurate term "cybersentinel";

Notes that the European Court of Auditors, in its aforementioned opinion 02/2023, stated that the present proposal was likely to "make the whole European Union cybersecurity galaxy more complex" and specified that there was a risk of "overlap between the existing CSIRT network and the SOCs";

Emphasises also that the Nevers Call from the European Union ministers responsible for telecommunications, published on 9 March 2022 under the French Presidency of the Council of the European Union (FPEU), encouraged strengthening European cooperation and solidarity in cybersecurity by building on existing networks;

Recalls in this respect the need for local authorities, administrations and businesses to anticipate cybersecurity crises by drawing up a business continuity plan (BCP);

Considers, finally, that if the European cybersecurity architecture is to be fully effective, it must be easily understood by all players in society, citizens and businesses alike;

Calls for the preservation of the existing European cybersecurity architecture and the strengthening of existing cooperation bodies;

Recommends, therefore, the withdrawal of the SOC mechanism, since it does not appear obvious that it is either necessary or relevant, and the explicit incorporation of its functions within the CSIRTs' remit; stresses the relevance of the regional level for responding to IT incidents referred to the CSIRTs; calls for the development of cooperation between regional CSIRTs in neighbouring Member States;

Questions the relevance of the European Commission's systematic presence in the exchanges of sensitive information provided for in Article 7 of the Proposal given its lack of operational competence in the field of cybersecurity and the fact that it already sits as an observer on the EU-CyCLONe network;

On the emergency mechanism

Whereas the present Proposal plans to create an emergency mechanism comprised mainly of a European cybersecurity reserve that will intervene in case of crisis upon the request of a Member State and the decision of the European Commission, and as a last resort;

Whereas the European cybersecurity reserve could also benefit, upon request, third countries that have appointed a single point of contact and provided sufficient information about their cybersecurity initiatives and capabilities;

Whereas the European cybersecurity reserve would be made up of private companies selected as trusted providers in calls for bids, subject to interested companies fulfilling technical skills criteria and data privacy guarantees;

Whereas the companies that intervene as part of the reserve framework would receive pre-funding intended to ensure they are available in case of incident and that, should these funds not be used, could be reallocated to preparedness initiatives;

Takes note of this emergency mechanism based on a public/private alliance, which is inspired by the French cybersecurity organisation set up around ANSSI; notes, however, that this model is the result of insufficient resources being allocated to the national authorities responsible for cybersecurity;

Takes note of the possibility for non-European companies to intervene within the European cybersecurity reserve in the critical infrastructures of a Member State facing a cybersecurity crisis; highlights that this possibility represents a non-negligible risk of foreign interference in these entities' operations; notes that the introduction of such a possibility reflects the European Union's current state of dependency; observes that this dependency cannot continue in the light of the European Union's strategic autonomy ambitions;

Recommends, therefore, that only service providers with their registered office in the European Union, the European Economic Area or a third country associated with the European Union and party to the World Trade Organisation (WTO) Agreement on Government Procurement should be included in the reserve;

Calls, therefore, on the European Union to support European service providers and foster their "ramping up" as a means to guarantee its strategic autonomy; calls, in addition, for an increase in ENISA's resources through a recruitment plan for European cyber-experts; adds that France must itself continue to enhance its ability to prevent and respond to cyber-attacks;

Calls, furthermore, for the proposed mechanism to require the Member States to lay down effective, proportionate and dissuasive penalties to punish the theft, the unauthorised dissemination of confidential information and the espionage that could result from triggering the emergency mechanism;

Notes that Article 17 of this Proposal provides that the European cybersecurity reserve could also intervene in a third country associated with the European Union, at the request of that country and provided that the association agreement signed

between the two parties mentions such an intervention; considers it necessary, however, to specify in this Proposal the arrangements for the reserve's intervention in the event of simultaneous requests from Member States and third countries, providing first and foremost for priority to be given to Member States and then to third countries which are candidates for accession to the European Union;

On the analysis mechanism for cybersecurity incidents

Whereas the aim of the proposal is to entrust ENISA with the task of analysing cybersecurity incidents, at the request of the European Commission, the EU-CyCLONe network and the CSIRT network;

Approves the idea of such a mechanism to promote coordination between the relevant bodies, giving them the mutual benefit of "feedback" on crises so they can draw lessons for the future;

Points out, however, that the NIS 2 directive already entrusts such a task to the EU-CyCLONe network and therefore suggests that the wording of the proposed mechanism be clarified in order to avoid "doubling up";

Seeks confirmation that the Member States will be fully involved in ENISA's review of cybersecurity incidents by contributing to incident analysis and being informed of the conclusions of analysis;

On the scale of reliance on implementing acts

Notes that Article 291 of the Treaty on the Functioning of the European Union (TFEU) provides for the use of implementing acts; stresses that such use is justified where uniform conditions for implementing legally binding acts of the European Union are needed; notes, however, that by defining in implementing acts both the types and number of "incident response services" needed to trigger the European Union's cybersecurity reserve and the procedures for awarding the support services provided by that

reserve, Articles 12 and 13 of the proposal give the European Commission undue executive powers;

On European institutions' level of cybersecurity preparedness

Recalls that in 2022 the European Court of Auditors found that European institutions' cybersecurity preparedness was "overall not commensurate" with the threats, highlighting in particular the lack of guidelines and operational protocols, as well as the scarcity of training provided to their staff;

Welcomes, therefore, the final adoption of the Proposal for a Regulation COM(2022) 122 final laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.