Council of the European Union

Brussels, 16 November 2023
(OR. en)

15565/23

Interinstitutional File:
2023/0109(COD)

LIMITE

CYBER 292
TELECOM 338
CADREFIN 173
FIN 1174
BUDGET 41
IND 605
JAI 1500
MI 993
DATAPROTECT 318
RELEX 1330
CODEC 2169

NOTE

From:	Presidency
To:	Delegations
Subject:	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 - Progress Report

The Presidency has drawn up a progress report on 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, the "EU Cyber Solidarity Act", in order to report on the work carried out so far by the Council preparatory bodies and on the state of play in the examination of the proposal.

ANNEX

INTRODUCTION

1. On 18 April 2023, the Commission adopted 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, the "EU Cyber Solidarity Act". EU Cybersecurity Strategy adopted in December 2020 mentioned the creation of a European Cyber Shield, reinforcing the cyber threat detection and information sharing capabilities in the European Union. The Council Conclusions of October 2021 highlighted the need to address gaps in terms of response and preparedness to cyber-attacks, by calling for the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity. Finally, on 8 and 9 March 2022, Ministers of EU Member States in charge of Telecom issues met informally in Nevers and expressed the wish to reinforce the support to national efforts of Member States victims of cyber-attacks.

2. The purpose of this proposal is - among others - to strengthen the competitive position of industry and service sectors and support their digital transformation. The proposal aims at increasing the resilience of citizens, businesses and entities operating in critical and highly critical sectors against the growing cybersecurity threats with societal and economic impacts. The legal basis is therefore Article 173 TFEU on competitiveness as well as Article 322 (1) point (a) TFEU on carry-over rules derogating from the principle of budget annuality. The latter legal basis is necessary to the establishment of a Cybersecurity Emergency Mechanism. Other objectives of this Regulation are: to strengthen common EU detection and situational awareness of cyber threats and incidents; to reinforce preparedness of critical entities across the EU and strengthen solidarity by developing common response capacities against significant or large-scale cybersecurity incidents, including by making incident response support available for third countries; to enhance Union resilience and contribute to effective response by reviewing and assessing significant or large-scale incidents.

3. In particular, the proposal lays down:

   – The deployment of a pan-European infrastructure of Security Operation Centers (SOCs) (European Cyber Shield) to build and enhance common detection and situational awareness capabilities.

   – The creation of a Cyber Emergency Mechanism to support Member States in preparing for, responding to and immediate recovery from significant and large-scale cybersecurity incidents.

   – The establishment of a European Cybersecurity Incident Review Mechanism to review and assess specific significant or large-scale incidents.

STATE OF PLAY OF WORK WITHIN THE COUNCIL PREPARATORY BODIES

4. Under Swedish presidency the Commission presented the text at meeting of the Horizontal Working Party on Cyber Issues (HWPCI) on 24 April 2023, and then had thematic presentations on 24 May and 7 June 2023.

5. Under Spanish Presidency, the HWPCI had an exchange of views on 10 July and 18 September, followed by an explanatory workshop organised by the Presidency on SOCs and their role, with the attendance of the experts from capitals. A read through of the text took place on 18 September. Further clarifications were presented by the Commission on 25 September. Following these exchanges, the Presidency presented a first compromise proposal on 2 October 2023.

6. This compromise proposal mainly tackled articles and provide for solutions to Member States concerns. In particular, the text clarifies terminology and adapts it to the requests of Member States (in particular on SOCs and the Cyber Shield). Also, in the subject matter and scope, language was improved on the response measures and recovery as well as provisions referred to national security. Definitions have been modified and aligned with other legislation, mainly NIS2 Directive. The voluntary nature of the involvement of Member States in the mechanisms established by the Regulation was stressed throughout the text. In general, relations between the existing entities and the ones defined by the Regulation have been clarified. Improvements have been introduced on procurement, funding, information sharing and the incident review mechanism.

7. HWPCI discussed the first compromise proposal on the meetings of 2 and 9 of October and had an exchange on the Cyber Reserve, budgetary aspects and the role of CSIRTs/SOCs on 23 October. On 16 October, a workshop was organised by the Commission, to further clarify practical aspects of the Cyber Reserve. Following these meetings, the Presidency presented a second compromise proposal on 3 November.

8. The second compromise text clarifies further the interaction of the entities defined in the proposal with the existing structures. Suggestions on trusted providers and the support to third countries have been integrated to the extent possible. Language on the voluntary nature of the activities has been further strengthened. The HWPCI discussed this compromise text on 6 and 13 November. Member States shared their concerns on: the risk of duplication between the SOCs and CSIRTs activities as well as related terminology, role of existing structures, including ENISA, the functioning of the Reserve, the importance to integrate preparedness in the activities of the Reserve, the management of support action to third countries, liability and the services provided in the Regulation.

9. The Presidency plans to continue these discussions in the coming weeks and remains determined to obtain a mandate.

10. On the basis of the progress made under the Spanish Presidency, the incoming Belgian Presidency plans to continue the work with the Parliament on this important file.

11. In the light of the above, the Permanent Representatives Committee and the Council are invited to take note of the progress made on the examination of the proposal for a Regulation.