Council of the European Union

Brussels, 8 October 2021
(OR. en)

12534/21

CYBER 253
JAI 1064
TELECOM 361
CSC 340
CIS 110
RELEX 827
ENFOPOL 343
COPS 341
COSI 179
HYBRID 59
CSCI 127
POLGEN 172
DATAPROTECT 230

'I/A' ITEM NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee (Part 2)/Council
Subject:	Council Conclusions on exploring the potential of the Joint Cyber Unit initiative - complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises - Approval

1. On 23 June 2021, the Commission published its Recommendation on building a Joint Cyber Unit[1] to tackle the rising number of serious cyber incidents impacting public services, as well as the life of businesses and citizens across the European Union.

2. The Commission presented the Recommendation in the Horizontal Working Party on Cyber Issues (HWPCI) on 28 June 2021. Subsequent discussions took place under the Slovenian Presidency during the HWPCI meetings on 7 and 14 July 2021 to gather Member States' views on the Commission Recommendation.

[1] C(2021) 4520 final (11155/21 and 11155/21 ADD1).

3. The Presidency presented a first draft of the Council conclusions on exploring the potential of the Joint Cyber Unit initiative - complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises[2] at the informal videoconference of the members of the HWPCI on 23 July 2021. These draft conclusions were further discussed in the meetings of the members of the HWPCI on 8 and 29 September 2021.

4. During its meeting on 6 October 2021, the HWPCI agreed on the draft Council conclusions as set out in the Annex.

5. In view of the above, the Permanent Representatives Committee is invited to submit the draft Council conclusions, as set out in the Annex, to the Council and to suggest that it adopts these draft conclusions as an 'A' item on its agenda.

---

[2] 10975/21.

ANNEX

Draft Council conclusions on exploring the potential of the Joint Cyber Unit initiative - complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises

THE COUNCIL OF THE EUROPEAN UNION,

RECALLING its conclusions on:

– the EU's Cybersecurity Strategy for the Digital Decade[3],

– the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises[4],

– Cyber Diplomacy[5],

– a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox')[6],

– Security and Defence[7],

– the EU Cyber Defence Policy Framework[8],

– Shaping Europe's Digital Future[9],

– Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements,

---

3 7290/21.
4 10086/18.
5 6122/15 + COR 1.
6 10474/17.
7 8396/21.
8 15585/14.
9 8711/20.

– the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU[10],

– cybersecurity capacity and capabilities building in the EU[11],

1. EMPHASISES the importance of cybersecurity for building a resilient, digital and green Europe. STRESSES that cybersecurity is indispensable for the prosperity and security of the EU and its Member States, its people, businesses and institutions, as well as for upholding the integrity of our free and democratic societies.

2. ACKNOWLEDGES the cross-border and cross-sectoral nature of many cybersecurity threats, and the risks and potential implications of the continuous campaigns of more impactful, sophisticated, targeted, complex, persistent, and/or pervasive malicious cyber activities[12]. The COVID-19 pandemic has further exposed the vulnerabilities of our societies and the potential for damage from large-scale cyber-incidents to the economy, democracy, essential services and critical infrastructure, most notably in the health sector. It has also increased the importance of connectivity and society's dependence on reliable, trustworthy and secure network and information systems. Ultimately, it has underlined the need for a global, open, free, stable and secure internet, as well as for trust in information and communication technology (ICT) products, processes and services and their security, including the need to ensure a resilient supply chain.

---

10 14435/17 + COR 1.
11 7737/19.
12 ENISA Threat Landscape 2020.

3. REITERATES the importance of cyber resilience and further developing the EU's cybersecurity crisis management framework[13] aiming at an efficient and timely response at EU level to large-scale cybersecurity incidents and crises, and further integrating it into existing horizontal and sectoral EU crisis response mechanisms. STRESSES the role of the Council and the Integrated Political Crisis Response (IPCR) arrangements in ensuring timely coordination and response at Union political level for crises, whether they originate inside or outside the Union, and which have a wide-ranging impact or political significance. HIGHLIGHTS the importance of testing such frameworks and mechanisms in regular exercises.

4. RECALLS that activities at EU level with regard to large-scale cyber incidents and crises take place in accordance with the principles of subsidiarity, proportionality, complementarity, non-duplication, and confidentiality. REITERATES that Member States have primary responsibility for the response to large-scale cybersecurity incidents and crises affecting them. RECALLS the importance of respecting the competences of the Member States, and their sole responsibility for national security, in accordance with Article 4(2) of the Treaty on European Union, including in the domain of cybersecurity.

5. RECALLS at the same time the importance of respecting the competences and mandates of the EU institutions, bodies and agencies. The High Representative, the Commission and other EU institutions, bodies and agencies also have an essential role to play, stemming from Union law, including owing to the possible impact of large-scale cybersecurity incidents and crises on the single market, as well as on the functioning of the EU institutions, bodies and agencies themselves.

[13] 10086/18.

6. UNDERLINES the need to avoid unnecessary duplication and to seek complementarity and added value in the further development of the EU cybersecurity crisis management framework, and to ensure alignment with existing mechanisms, initiatives, networks, processes and procedures at national and European level. EMPHASISES the importance of streamlining existing processes and structures to reduce complexity, and in the interest of cohesion in the Union to improve accessibility and responsiveness to those who seek assistance and solidarity.

7. RECOGNISES the applicability of international law, including the United Nations Charter in its entirety, international humanitarian law and human rights law in cyberspace, and PROMOTES adherence to the voluntary, non-binding norms, rules and principles of responsible state behaviour in cyberspace endorsed by all UN Member States.

8. WELCOMES the progress achieved in recent years within the Council, in particular in the Horizontal Working Party on Cyber Issues (HWPCI) and other relevant Council working groups, as well as in setting up other cooperation and information sharing initiatives, networks and mechanisms among Member States, notably the NIS Cooperation Group and the CSIRTs Network, set up by Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, the Cyber Crises Liaison Organisation Network (CyCLONe), as well as relevant cyber defence-related projects launched under the Permanent Structured Cooperation (PESCO)[14], the Joint Cybercrime Action Taskforce (J-CAT), the European Judicial Cybercrime Network (EJCN), Member States' voluntary contributions to EU INTCEN, and coordination and cooperation in the context of the Cyber Diplomacy Toolbox.

[14] In particular, the "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security" coordinated by Lithuania, the "Cyber and Information Domain Coordination Centre" coordinated by Germany, "Cyber Threats and Incident Response Information Sharing Platform" coordinated by Greece.

9. RECALLS the existing frameworks for cooperation among EU institutions, bodies and agencies, such as the structured cooperation between ENISA and CERT-EU, and the Memorandum of Understanding between ENISA, the European Defence Agency (EDA), Europol's European Cybercrime Centre (EC3) and CERT-EU. STRESSES the importance of continued regular information sharing with the Council on further developments in these frameworks of cooperation.

10. HIGHLIGHTS the importance of enhancing cooperation and information-sharing amongst the various cyber communities within the EU and its Member States at all necessary levels – technical, operational and strategic/political - and of linking existing crisis management mechanisms, networks, structures, processes and procedures where this supports and improves the handling of large-scale cyber incidents and crises.

11. ACKNOWLEDGES the progress achieved by a group of Member States in the creation of a joint operational cyber capability 'Cyber Rapid Response Teams' under the PESCO framework aiming to deepen voluntary cooperation in the cyber field through mutual assistance, including in response to large-scale cyber incidents and crises.

12. ACKNOWLEDGES the experience and 24/7 response capability of the law enforcement community in the area of operational cooperation and secure information exchange against major cross-border cyber-attacks through the EU Law Enforcement Emergency Response Protocol.

13. RECOGNISES the continued implementation of the framework for a joint EU diplomatic response to malicious cyber activities ('Cyber Diplomacy Toolbox'). RECALLS that every Member State is free to make its own sovereign decision with respect to the attribution of a malicious cyber activity taken on a case-by-case basis. RECALLS that the measures taken within the framework for a joint EU diplomatic response to malicious cyber activities should be based on a shared situational awareness agreed among Member States. EU INTCEN plays a central role as the hub for the provision of situational awareness and threat assessment on cyber issues for the EU, based on voluntary intelligence contributions from the Member States and without prejudice to their competences.

14. REITERATES the importance of mutual assistance and solidarity, in line with Article 42(7) of the Treaty on European Union and Article 222 of the Treaty on the Functioning of the European Union, and CALLS for further exercises with a cyber dimension. RECALLS the need to reflect on the articulation between the EU cybersecurity crisis management framework, the Cyber Diplomacy Toolbox and the provisions of the above mentioned articles in case of a large-scale cyber incident or crisis. RECALLS further that obligations for the Member States stemming from Article 42(7) of the Treaty on European Union are without prejudice to the specific character of the security and defence policy of certain Member States. RECALLS as well that NATO remains the foundation of their collective defence for those States which are members of it.

15. ACKNOWLEDGES the EU-NATO cooperation on cyber security and defence, including information sharing between CERT-EU and NATO Computer Incident Response Capability (NCIRC), in full respect of the principles of transparency, reciprocity and inclusiveness as well as the decision-making autonomy of both organisations.

16. ACKNOWLEDGES the importance of cooperation, when appropriate, with the private sector in terms of information sharing exercises, and the provision of relevant expertise, as well as trusted solutions and services, including for example in supporting incident response and bolstering situational awareness between different cyber communities.

17. STRESSES the importance of secure communication channels for the exchange of classified and sensitive information. HIGHLIGHTS the need for further progress.

In this regard, and taking into account the above,

18. ACKNOWLEDGES the Commission Recommendation on building a Joint Cyber Unit, as an initiative to be considered in further developing the EU cybersecurity crisis management framework[15].

19. CALLS upon the EU and its Member States to continue their efforts towards a more comprehensive and effective EU cybersecurity crisis management framework, building on existing mechanisms and on the progress already achieved, and to take into consideration the potential of the Joint Cyber Unit initiative to complement these mechanisms by taking a step-by-step approach. STRESSES that an incremental, transparent and inclusive process is essential for enhancing trust and, therefore, critical to the further development of an EU cybersecurity crisis management framework. This process should respect the existing roles, competencies and mandates of the Member States and EU institutions, bodies and agencies, as well as the principles stated in these conclusions, including proportionality, subsidiarity, inclusivity, complementarity, non-duplication, and confidentiality of information. STRESSES, at the same time, that any possible participation in or contributions by Member States to a potential Joint Cyber Unit are of a voluntary nature.

[15] C(2021)4520 final (11155/21 and 11155/21 ADD1).

20. STRESSES the need to establish adequate working methods and governance, with a view to allowing for the involvement and participation of all Member States in the deliberations, development and effective decision-making processes on the EU cybersecurity crisis management framework, including on the potential Joint Cyber Unit initiative. CALLS for the Council's prerogatives under the Treaties and the principle of sincere cooperation to be respected.

21. UNDERLINES the importance of identifying and involving all relevant cyber communities within the EU and its Member States, while considering their different roles and responsibilities in different types of large-scale cyber incidents and crises. UNDERLINES the instrumental role of the Council, in particular through the HWPCI, in the policy-making and coordination function with regard to further developing the EU cybersecurity crisis management framework. INVITES, therefore, the Member States, the Commission, the European External Action Service (EEAS), EU INTCEN, CERT-EU, ENISA, Europol (EC3), Eurojust (EJCN), the European Cybersecurity Industrial, Technological and Research Competence Centre (ECCC), as well as representatives from the CSIRTs Network, CyCLONe, the NIS Cooperation Group, the EDA, and relevant PESCO projects, as well as other possible stakeholders, to engage in this process. A possible working group, as proposed in the Commission Recommendation, could be explored further, by ensuring adequate representation of all Member States and acting under the political guidance of the Council, to serve as a temporary forum bringing together representatives of all relevant cyber communities in the Member States and within the EU. Such working group should regularly report on its activities and submit possible suggestions to the Council for discussion, endorsement and further guidance. In addition, other forms of dialogue within and across communities could be established, including through workshops, seminars, joint training and exercises.

22. UNDERLINES the role for the European Cybersecurity Industrial, Technological and Research Competence Centre (ECCC) and the Network of National Coordination Centres in relation to the potential Joint Cyber Unit, especially considering its role to substantially increase the Union's technological capacities, technological solutions, capabilities and skills in the area of cybersecurity.

23. INVITES the EU and its Member States to engage in further developing the EU cybersecurity crisis management framework, including by exploring the potential of a Joint Cyber Unit initiative, by setting and defining the process, including milestones and a timeline, as well as clarifying the aims and possible roles and responsibilities. EMPHASISES the need to consolidate, as a matter of priority, existing networks and interactions within each community, as well as to establish a thorough mapping of possible information sharing gaps and needs within and across cyber communities and also within and across European institutions, bodies and agencies, and subsequently agree on possible primary objectives and priorities of a potential Joint Cyber Unit. Without prejudging the outcome, STRESSES the need to focus on the identification of information sharing needs in order to build a common situational awareness among all relevant communities. In the identification of information sharing gaps and needs, including the possible use of virtual platforms, due attention should continue to be given to secure communication channels for the exchange of classified and sensitive information, while STRESSING the importance of using already existing infrastructure. The introduction of a gradual approach is intended to build trust and a basis for possible further steps related to enhancing preparedness and operational cooperation. ACKNOWLEDGES that different objectives might warrant different solutions and the engagement of a different set of representatives of relevant cyber communities within the EU and its Member States.

24. CALLS for further consideration on a legal basis for the potential Joint Cyber Unit throughout the entire process, including an assessment of the tasks and roles vis-à-vis those assigned to ENISA in the Recommendation in light of Article 7 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019. CALLS for further reflection on individual elements of the Recommendation on the Joint Cyber Unit, including with regard to the idea of the EU Cybersecurity Rapid Reaction Teams, and to the EU Cybersecurity Incident and Crisis Response Plan. EMPHASISES that a potential Joint Cyber Unit has to respect the competences, mandates and legal powers of its possible future participants.

25. CALLS upon the EU and its Member States to consider the potential of a Joint Cyber Unit initiative, also from the perspective of the EU institutions, bodies and agencies in order to complement ongoing efforts at the level of Member States. WELCOMES the Commission's intention to reinforce the resilience of relevant EU institutions, bodies and agencies through its forthcoming Proposal for a Regulation on common binding rules on cybersecurity for EU institutions, bodies and agencies.

26. In conclusion, REITERATES its commitment to enhancing cyber resilience and further developing the EU cybersecurity crisis management framework and WILL REGULARLY MONITOR progress and provide further guidance for complementing the EU cybersecurity crisis management framework.