Council of the European Union

Brussels, 4 August 2021
(OR. en)

11155/21
ADD 1

CYBER 218
JAI 904
TELECOM 307
CSC 300
CIS 99
RELEX 702
ENFOPOL 299
COPS 298
COSI 155
HYBRID 52
CSCI 115
POLGEN 151
DATAPROTECT 200

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	2 August 2021
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	C(2021) 4520 final
Subject:	ANNEX to the COMMISSION RECOMMENDATION on building a Joint Cyber Unit

Delegations will find attached document C(2021) 4520 final.

Encl.: C(2021) 4520 final Annex

EUROPEAN
COMMISSION

Brussels, 23.6.2021
C(2021) 4520 final

ANNEX

ANNEX

to the

COMMISSION RECOMMENDATION

on building a Joint Cyber Unit

ANNEX - STEPS FOR BUILDING THE JOINT CYBER UNIT

This Annex further describes the core and supporting actions needed to establish and operationalise the Joint Cyber Unit.

1. *Step 1 – Assessment of the Joint Cyber Unit's organisational aspects and identification of available EU operational capabilities*

CORE ACTIONS

Operational participants of the Joint Cyber Unit, gathered in a Working Group set up by the Commission and with the support of ENISA, should gather information about existing operational capabilities, including a list of available recognised professionals with an indication of their relevant expertise, available incident handling tools, functions and assets, available training and exercise portfolios, and existing information and intelligence analysis products. Based on that input, operational participants should prepare **a list of available EU operational capabilities** ready to be deployed in case of cyber incidents or crises, notably through EU Cybersecurity Rapid Reaction teams.

The working group should launch an assessment of **organisational aspects of** the Joint Cyber Unit **and the roles and responsibilities of operational participants within that platform**.

In order to acquire an overview of capabilities and agree on procedures, core and, to the extent possible, supporting actions under step one should be completed by **31 December 2021 [6 months after adoption]**.

2. *Step 2 – Preparing Incident and Crisis Response Plans and roll-out joint preparedness activities*

CORE ACTIONS

Operational participants in the working group, in consultation with supporting participants, should prepare the **EU Cybersecurity Incident and Crisis Response Plan** on the basis of the national Cybersecurity Incident and Crisis Response Plans. The EU Cybersecurity Incident and Crisis Response Plan should include objectives of EU preparedness, identified procedures and secure information exchange channels, including ways of handling information, as well as criteria for activating the mutual assistance mechanism based on an agreed incident classification taxonomy and on the list of available EU capabilities.

By the end of step two, the working group should conclude its assessment of the organisational aspects of the Joint Cyber Unit and the roles and responsibilities of operational participants within that platform. The working group should present the results of that assessment to the

Commission and the High Representative. The Commission and the High Representative should share such assessment with Council. The Commission and the High Representative should work together, in line with their respective competencies, to draw up a joint report based on that assessment and invite the Council to endorse that report via Council conclusions.

SUPPORTING ACTIONS

The EU Cybersecurity Incident and Crisis Response Plan should build on the main elements of national Cybersecurity Incident and Crisis Response Plans. In line with the Commission's proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 [1], Member States should adopt national Cybersecurity Incident and Crisis Response Plans. The national plans, which may possibly be subject to peer review, should define objectives and modalities in the management of large scale cybersecurity incidents and crises. The national plans should address, in particular, the following issues:

a. objectives of national preparedness measures and activities;
b. roles and responsibilities of the national competent authorities at national level;
c. national crisis management procedures and information exchange channels;
d. the identification of preparedness measures, including exercises and training activities;
e. the identification of relevant public and private stakeholders and infrastructure involved;
f. the national procedures and arrangements between relevant national authorities and bodies, including those responsible for all cyber communities, to ensure Member State effective participation in and support to the coordinated management of large-scale cybersecurity incidents and crises at EU level.

Based on the input provided by Member States and EU institutions, bodies and agencies, the operational participants should perform the following supporting actions within the framework of the Joint Cyber Unit:

a. set the first EU Integrated Situational report building on national Cybersecurity Incident and Crisis Response Plans;
b. establish communication capabilities and secure information sharing tools;
c. facilitate the adoption of protocols for mutual assistance among participants;
d. organise cross-community exercises and trainings for experts included in the list of EU available operational capabilities;
e. develop a multi-annual plan to coordinate exercises.

When needed, operational participants should consult supporting participants. ENISA, with the support of the Commission, Europol and CERT-EU, should enable information sharing by establishing communication capabilities and secure information sharing tools.

[1] COM(2020) 823 final 2020/0359 (COD), Brussels, 16.12.2020.

To ensure that the necessary plans are set-out and joint activities start to be rolled-out, core and, to the extent possible, supporting actions under step two should be completed by **30 June 2022 [6 months after the end of step 1]**.

3. *Step 3 – Operationalising the Joint Cyber Unit*

CORE ACTIONS

Following the Council's endorsement of the Commission's conclusions on the report under step two, operational participants should coordinate the deployment of **EU Cybersecurity Rapid Reaction teams** within the Joint Cyber Unit and establish a **physical platform** for allowing teams to carry out technical and operational activities. Based on the preparatory work carried out under step two, participants should finalise the EU Cybersecurity Incident and Crisis Response Plan. Operational participants should make sure that the experts and capabilities included in the list of EU available operational capabilities are available and ready to contribute to the activity of EU Cybersecurity Rapid Reaction teams.

In order to implement the EU Cybersecurity Incident and Crisis Response Plan, participants should define an annual work programme.

SUPPORTING ACTIONS

The Joint Cyber Unit may be used by the cyber diplomacy community to align public communication. The platform may allow participants to contribute to political attribution as well as attribution within the criminal justice framework employed at police and judicial level. In addition, it may facilitate recovery and allow for structured synergies with national and cross-border monitoring and detection capabilities.

To ensure the operationalisation of the Joint Cyber Unit, core and, to the extent possible, supporting actions under step three should be completed by **31 December 2022 [6 months after the end of step 2]**.

4. *Step 4 – Expanding the cooperation within the Joint Cyber Unit to private entities and reporting on progress made*

CORE ACTION

Participants in the Joint Cyber Unit should draw up an activity **report on progress made in the implementation of the four steps set out in the Recommendation, describing achievements and challenges faced**. That report should include statistical information regarding operational cooperation activities carried out throughout the four steps. The report should be submitted to the Commission and the High Representative.

SUPPORTING ACTIONS

In order to extend the capabilities and information available to EU Cybersecurity Rapid Reaction teams, participants should ensure that the Joint Cyber Unit assists in the conclusion **of information-sharing and operational cooperation agreements between participants and private sector** entities providing, among others, threat intelligence and incident response services. They should also ensure, among other activities, that the Joint Cyber Unit supports in regular dialogue and information sharing activities on threats and vulnerabilities with users of cybersecurity solutions, primarily those under the scope of the NIS Directive or gathered in **EU-level Information Sharing and Analysis Centres (ISACs).**

Member States should support entities operating within their territory, in particular those under the scope of the NIS Directive, in having access and contributing to public-private dialogues with EU-level ISACs.

To guarantee a proper involvement of the private sector, core and, to the extent possible, supporting actions under step four should be completed by **30 June 2023 [6 months after the end of step 3]**.

HOW TO SWIFTLY MOBILISE EU OPERATIONAL CAPABILITIES

WHO PROVIDES CAPABILITIES: Operational participants

WHO MANAGES THE CAPABILITIES: Participants, within the Joint Cyber Unit, in line with agreed roles and responsibilities

Step	Objective	Task	Core action	Supporting action
Step 1 - Define by **31 December 2021 [6 months after adoption]**	PREPAREDNESS	**Identify capabilities**	**Operational participants to establish a list of EU available operational capabilities.**	
Step 2 - Prepare by **30 June 2022 [6 months under the end of step 1]**	PREPAREDNESS	**Define relevant procedures and arrangements to activate capabilities in case of need**	**Operational participants to prepare the EU Cybersecurity Incident and Crisis Response Plan (EU Cybersecurity Crisis Response Framework under the Blueprint), based on adopted national Plans**	**Operational participants to develop EU Integrated Situational reports based on the EU Cybersecurity Technical Situation report**
	PREPAREDNESS	**Exercise capabilities**		**Participants to organise joint exercise and training (cross-community)** **Participants to work on a multi-annual plan to coordinate exercises.**

	SITUATIONAL AWARENESS	**Establish tools to share information and requests of support**		**Participants to develop secure and rapid information-sharing**
JCU IS OPERATIONAL **Based on the preparatory work carried out by participants under a Working Group to be set up by the Commission**				
Step 3 – Deploy by **31 December 2022 [6 months after the end of step 2]**	PREPAREDNESS	**Adopt relevant procedures, arrangements and memoranda of understanding to activate capabilities in case of need**	**Operational participants to finalise the EU Cybersecurity Incident and Crisis Response Plan and define its implementation through annual work programmes.**	**Participants to support to the establishment national and cross-border monitoring and detection capabilities, including the establishment of SOCs**
	COORDINATED RESPONSE	**Deploy capabilities in case of need**	**Operational participants to coordinate operational EU Cybersecurity Rapid Reaction teams through the JCU virtual and physical platform in Brussels.**	**Participants to coordinate public communication and contribute to political attribution, as well as attribution in the context of the criminal justice**
Step 4 – Expand and Report by **30 June 2023 [6 months after the end of step 3]**	SITUATIONAL AWARENESS	**Ensure scalability by involving the private sector to provide for emerging needs**	**Participants to submit an activity report about progress made, describing achievements and challenges with the support of statistical information.**	**Participants to conclude information-sharing agreements, as well as operational cooperation agreements with cybersecurity providers**
	COORDINATED RESPONSE			**Participants to conclude information sharing agreements with cybersecurity users, primarily entities under the NIS Directive scope and EU-ISACs**

CERTIFIED COPY
For the Secretary-General

Martine DEPREZ
Director
Decision-making & Collegiality
EUROPEAN COMMISSION