Council of the
European Union

Brussels, 13 December 2021
(OR. en)

14975/21

LIMITE

CYBER 329
JAI 1412
TELECOM 462
CSC 443
CIS 133
RELEX 1092
ENFOPOL 513
COPS 474
COSI 251
HYBRID 80
CSCI 157
POLGEN 202
DATAPROTECT 293

NOTE

From:	Presidency
To:	Horizontal Working Party on cyber issues
Subject:	Exploring the potential of the Joint Cyber Unit: 2021 Report and possible next steps

Delegations will find attached a Presidency paper on the above topic for the Horizontal Working Party meeting on 14 December 2021.

ANNEX

PRESIDENCY PAPER ON EXPLORING THE POTENTIAL OF THE JOINT CYBER UNIT - 2021 REPORT AND POSSIBLE NEXT STEPS

Following the adoption 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 (19 October 2021), as well as the Presidency paper on the way forward from 20 October 2021 (13019/21), the Presidency outlines hereby **a short summary of the progress achieved by mid-December and possible next steps for 2022, which can serve as a food for thought in further discussions on exploring the potential of the Joint Cyber Unit Initiative**.

a) Horizontal Working Party on Cyber Issues, NIS Cooperation Group, CyCLONe, CSIRTs Network

The Horizontal Working Party on Cyber Issues discussed the Presidency paper and recommendations on the next steps (13019/21) on 20 and 27 October 2021. Following these discussions, the Chair of the Horizontal Working Party on Cyber Issues invited the Chairs of the CSIRTs Network, CyCLONe and the NIS Cooperation Group to discuss in their respective meetings "mapping of information sharing gaps and needs, as well as tools, within and across communities" in line with the Council conclusions and the Presidency paper. **A joint CSIRTs Network and CyCLONe meeting took place on 11 November and the NIS Cooperation Group met on 25 November. The Presidency gave a debriefing of the discussions at these meetings at the Horizontal Working Party on Cyber Issues on 1 December 2021.**

Some of the conclusions of these November meetings are the following (as summarised by the Presidency):

- further efforts are needed to map the information sharing and situational awareness gaps to be able to identify the necessary solutions;
- Member States remain committed to the ideas and principles, as enshrined in the Council conclusions, as guidance for further work;
- Member States are encouraging the efforts at EU level to focus especially on the EU institutions, bodies and agencies, to complement the work already achieved at the level of the Member States, while they are also committed to enhance cooperation and exchanges at the national level.

Some of the proposed areas of work as part of the next steps included:

- a national point of contact for the Joint Cyber Unit; as well as the idea of a directory of different national points of contact representing different communities in Member States and EU institutions, bodies and agencies,
- the idea of using the Joint Cyber Unit as a tool to promote consolidated analysis and reports, while recognising at the same time that there are different needs, roles and responsibilities of communities involved; sometimes also different timelines of engagement;
- the idea of creating a single document describing procedures of individual communities aimed at improving common understanding about the procedures, roles and responsibilities (a possible handbook); while recognising that efforts are already ongoing in the framework of CyCLONe;

- the necessity of further exercises within and across communities of Member States and EU institutions, bodies and agencies;
- the idea of bringing concrete business cases for the Joint Cyber Unit, possibly based on previous real life experience of cooperation within and across communities;
- ideas on modalities of further work, including the idea for a greater engagement of the NIS Cooperation Group Work Stream 7 (on large scale incidents and crises); while recognizing that such a setting might not enable cooperation of all communities, but would focus only on certain aspects; as well as the idea of a separate working group offering broader engagement of all communities etc.

b) Workshops

In addition, **following the adoption of the Council conclusions, two workshops organised by ENISA took place**.

The first workshop was dedicated to the topic of situational awareness in EU Institutions, bodies and agencies and was held on 26 October. ENISA, INTCEN, CERT-EU, Europol, and EDA presented their experiences and initiatives. The Presidency sees positively these efforts made by the EU Institutions, bodies and agencies to enhance their exchange of information and situational awareness and encourages continuation of this valuable work.

The second workshop was held on 7 December and focused on Member States and their experiences and initiatives related to the identification of information sharing gaps and needs in order to build situational awareness. Among others, Member States shared how they have built cross community exchanges, lessons they have learned in their national processes, and tools that they are using. One of the prevailing messages was the importance of time that was necessary for building the necessary trust, as well as the importance of ensuring mutual understanding of the roles and responsibilities of the communities, as well as the need to ensure the necessary legal frameworks enabling such exchanges. The EU institutions, bodies and agencies also provided an update on their initiatives at the same event.

c) Exercises

Moreover, **the Presidency organised together with the EEAS a Cyber Diplomacy Toolbox tabletop exercise for the Horizontal Working Party on Cyber Issues on 17 November 2021**. The exercise indirectly contributed to the ongoing efforts in line with the Council conclusions from 19 October by promoting synergies and awareness raising with contributing participants from EU INTCEN, CERT-EU, Europol, ENISA, CSIRTs Network, CyCLONe and experts on the IPCR from the General Secretariat of the Council. The EDA, EUMS, Commission (DG CNECT, DG HOME, DG DIGIT), as well as NATO were invited as observers. This exercise, similar to those that were held at the level of CSIRTs Network and CyCLONe and within other communities, proved also as an **important element of the consolidation of the existing networks/communities, which is one of the steps in the implementation of Council conclusions**.

d) Summary of key discussions and recommendations for possible next steps

Regarding the identification and involvement of all relevant cyber communities within the EU and its Member States as actors to be involved in the process, Member States indicated in the Horizontal Working Party on Cyber Issues that the current identification as provided for in the Council conclusions is sufficient to proceed and can be complemented later in the process, if needed. The Presidency would encourage all relevant stakeholders **to consult the entities as mentioned in the Council Conclusions** for preparing the next steps. At the same time, the Presidency would like to **stress that each community has representatives of Member States and EU institutions, bodies and agencies**.

The majority of efforts so far focused on promoting dialogue and exchanges within and across cyber communities. Until today, the work achieved has already enabled involved actors from various communities to know more about each-other's communities, roles and procedures and situational awareness mechanisms. A more intensified dialogue was established, which has already led to greater **trust and the Presidency believes this work should continue**.

At the same time, the Presidency would like to point out that **further efforts are needed to ensure a more inclusive process involving all four communities** – cybersecurity, law enforcement, diplomacy and defence, while respecting each other roles and responsibilities.

Not all communities share the same level of cooperation at the EU level, which has to be considered in the next steps as well. For this reason, the Presidency proposes to **consider also possible separate or parallel strands of work** to be able to move forward on areas, where it is possible to already discuss and introduce some concrete steps forward.

Despite the understanding and acknowledgement of the general goal of the JCU to reinforce and enhance cyber crisis management by promoting greater information exchange for better situational awareness, **the discussions have so far demonstrated that there is still a need for more clarity on the objectives to be achieved by the potential Joint Cyber Unit**. This shall not hinder the process focused on achieving some first concrete steps forward, where possible.

The present paper aims at presenting possible next steps as options to be considered in order to better understand the objectives and implement concrete steps to continue to enhance information sharing processes and situational awareness.

Based on this, the Presidency, in consultation with the incoming French Presidency, recommends the following:

For situational awareness:

1. Building on the current effort on situational awareness by EU institutions, bodies and agencies, including the ENISA-CERT-EU structured cooperation, and in line with article 7 of the Cyber Security Act, continue working towards greater common cybersecurity situational awareness of the Union, including by means of consolidation and integration of information within the EU institutions, bodies and agencies, as well as from different communities and networks. The expected outcome could contribute to Union's preparedness and response to a cyber crisis or large-scale cross border incident. To this extent, proposals could be presented to the HWPCI as mean of consultation and update on the progress regarding:

   - Regular integrated reporting from the EU institutions, bodies and agencies contributing to common situational awareness (of the Member States and EU institutions, bodies and agencies),

   - Information sharing mechanisms and reporting during large-scale cyber incidents and crises to provide continuous situational awareness and information about the event and its impact on the Union during cyber crisis or large-scale – cross-border incidents.

   - Possible links between reports for EU institutions, bodies and agencies and existing Member States' networks should be considered.

2. **Member States and** relevant **EU institutions, bodies and agencies should explore** case studies of previous major incidents (for example: SolarWinds, Microsoft Exchange) to **identify further cross-communities gaps and based on this the needs** in terms **information sharing** for preparedness and response to Union cyber crises or large-scale cross-border incidents in order to determine possible areas for improvement.

As a first step and in this regard, the NIS Cooperation Group may consider identifying <u>from the civilian cyber security perspective</u> the perceived gaps in connecting to other communities. Possible other concrete steps, such as those in the point 6) could be also explored in the NIS Cooperation group for the civilian cybersecurity community. Invitations to other communities necessary to inform the work of the NIS Cooperation Group are encouraged.

3. **Presidency would encourage further** engagement **in exploring the potential of the Joint Cyber Unit, based on the Council conclusions, also in the law enforcement, cyber diplomacy and cyber defence communities, which were so far not yet fully included in the process**.

   Also these communities are invited to explore similar efforts as those that are outlined in point 2) above to build on concrete case studies, as well as to explore other steps, depending also specific characteristics of individual communities and level of engagement in the process so far. Possible invitations and exchanges with other communities to inform the work of the law enforcement, cyber diplomacy and cyber defence communities are encouraged as well.

4. **The Horizontal Working Party on Cyber Issues should be regularly informed on the planned next steps within or/and across communities** and **about the progress made** (such as those in points 2) and 3) above). Such information shall include inputs from all communities in order to enable a holistic overview of the Council.

5. **Based on the reports received, the Horizontal Working Party on Cyber Issues could, as one of the next steps, further consider the working arrangements for advancing the preparatory process exploring the potential of the Joint Cyber Unit**.

Further consideration could be given on how to engage in a more holistic manner all communities, and actors identified in Council conclusions: Member States, Commission, EEAS, EU INTCEN, CERT-EU, ENISA, EUROPOL (EC3), EUROJUST (EJCN), ECCC, relevant Member States Networks (such as CSIRT Network, CyCLONe), NIS Cooperation Group, EDA, relevant PESCO projects, as well as possible other stakeholders to engaged in this process.

The creation of a possible ad hoc working group could be explored further as a temporary working forum bringing together representatives of all relevant cyber communities (from Member States and EU institutions, bodies and agencies). It would have to be organised in a manner that provides a platform for the engagement of all stakeholders in line with their respective mandates. October Council conclusions can serve as guidance for this consideration as well. The ideas of points of contact could be considered in this regard as well. Regular meetings enabling all communities to come together may complement the efforts that are taking place or are planned to take place in individual communities.

6. In this regard and on this basis, the EU institutions, bodies and agencies jointly with Member States could consider also the following possible concrete steps in the future:

- Define taxonomy **and templates** with aligned assessment methodologies to be used during responses to large-scale cybersecurity incidents and crises.

- Update, where they exist, the **SOPs of each community** or explore other possible steps, to integrate and encourage cross-community sharing of information, and assess the need to elaborate possible common operational procedures that connect existing EU networks and EUIBAs operational procedures.

- Create a **directory of contact points** in the Member States and EUIBAs to be used during a large-scale cybersecurity incidents and crises.

- **Map existing information-sharing tools** that allow adequate level of protection of the exchanged information that could be used to exchange information.

- Continue with or establish other forms of dialogue within and across communities, including through workshops, seminars, informal discussions etc.

- Explore the possibility to organize a joint cross-community exercise or to include all communities **in periodic exercises,** such as CyberEurope.

- An important element for the future process are going to be **lessons and conclusions from the EU Cyber** Crisis **Linking Exercise Linking Exercise on Solidarity (EU CYCLES)** about improvements in cross-community cooperation in relation with the abovementioned steps as well as with regard to mutual assistance.

For operational cooperation:

While working on situational awareness, the Horizontal Working Party could start discussing in parallel a possible role for the potential Joint Cyber Unit initiative for operational cooperation.

e) **Concluding remarks**

In conclusion, the Presidency stresses that this report is not all encompassing in terms of ideas that were presented in the process so far, but rather a short summary with a proposal of possible further steps to advance work on complementing the EU cyber crisis management framework. Member States are invited to bring forward other ideas and possible further recommendations in the next steps of the process.

The state of play of the implementation and the proposed next steps will be discussed and assessed under the French Presidency of the Council of the EU, with a view to identifying concrete next steps in exploring the potential of the Joint Cyber Unit.