Council of the European Union
General Secretariat

Brussels, 28 July 2021

WK 9884/2021 INIT

LIMITE

CYBER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Spain contribution to the Joint Cyber Unit

Delegations will find in Annex Spain's contribution to the Joint Cyber Unit.

Spain contribution to Joint Cyber Security Unit

Considerations

According to Commission Recommendation of 23.06.2021 C(2021) 4520 final, on building a Joint Cyber Unit (JCU):

- Despite the major progress achieved through cooperation between Member States on cybersecurity, most notably through the Cooperation Group (‘NIS Cooperation Group’) and the Computer Security Incident Response Teams (CSIRTs) network set up under Directive (EU) 2016/11482, there is still no common EU platform where information gathered in different cybersecurity communities can be exchanged efficiently and safely and where operational capabilities can be coordinated and mobilised by relevant actors.
- Existing frameworks (Blueprint, CSIRTNW, CyCLONe, EC3, J-CAT, Europol, EDA, INTCEN, ENISA, IPCR, PESCO, ..), provide a strong basis for a collective response to cybersecurity threats, incidents and crises.
- However, mechanism for harnessing existing resources and providing mutual assistance across the cyber communities responsible for network and information systems security, for combating cybercrime, for conducting cyber-diplomacy, and, where appropriate, for cyber-defence in the event of a crisis does not yet exist.
- For this reason, the Commission, with the involvement of the High Representative, has developed a concept for a Joint Cyber Unit as a response to this analysis and as an important component of the Security Union Strategy, the Digital Strategy and the Cybersecurity Strategy.
- The Joint Cyber Unit provides for a virtual and physical platform and does not require the creation of an additional, standalone body. Its set-up should not affect the competencies and powers of national cybersecurity authorities and relevant Union entities.
- The Joint Cyber Unit should be anchored in memoranda of understanding between its participants.
- It should build on, and add value to, existing structures, resources and capabilities as a platform for secure and rapid operational and technical cooperation between EU entities and Member State authorities.
- Participants in the Joint Cyber Unit should focus on technical and operational cooperation, including joint operations.
- ENISA is in a unique position to organise and support the preparation of the Joint Cyber Unit, as well as to contribute to its operationalisation
- Member States and relevant EU institutions, bodies and agencies, building on ENISA’s contribution in accordance with Article 7(7) of Regulation 2019/881, should ensure a coordinated response to and recovery from large-scale incidents and crises …//… and should ensure that the Joint Cyber Unit provides continuous shared situational awareness and preparedness against cyber-enabled crises across cybersecurity communities.

Considering this Recommendation, the JCU will be based on **cooperation of all actors under a memoranda of understanding**.

Timeline and process

The JCU will move into operational phase on 30 June 2022, with operational capabilities and experts that form the basis of EU Cybersecurity Rapid Reaction teams and **fully completed by 30 June 2023**.

The creation of the Joint Cyber Unit should therefore follow a gradual and transparent process to be completed over the next two years in 4 steps:

- a. Step one - Assessment of the Joint Cyber Unit's organisational aspects and identification of available EU operational capabilities by 31 December 2021;
- b. Step two - Preparing Incident and Crisis Response Plans and rolling-out joint preparedness activities by 30 June 2022;
- c. Step three - Operationalising the Joint Cyber Unit by 31 December 2022; **The JCU will be operational**.
- d. Step four - Expanding the cooperation within the Joint Cyber Unit to private entities and reporting on progress made by 30 June 2023.

Resources

ENISA and the Commission should ensure the use of existing resources under the EU financing programmes, primarily the Digital Europe Programme.

Spanish position on JCU project

1. It is necessary to differentiate between a cybersecurity incident and a cybersecurity crisis. The procedures and actions to be developed start from a declared situation of alert, when usually, national CSIRTs (Technical level) and relevant authorities considered the situation caused by a cybersecurity incident is important enough to activate respective national mechanisms established to observe the evolution of the potential cybersecurity crisis.
2. In this regard, Member States would have to work out an appropriate escalation mechanism to crisis in more detail, from technical to operational level, and from operational to strategic/political. This mechanism should be also set up at European level, implementing Cyclone and supported by this Joint Cybersecurity Unit. Nowadays, in order to facilitate a coordinated response and to communicate as one voice during crisis and major incidents in the UE depends on achieving consensus within the framework of the actions developed for Blueprint. This would lead to a unique adoption of procedures, the construction of support tools for a coordinated crisis management and the adaptation of institutions in such a context.

3. The Blueprint gathers a three level (political, operational and technical) approach that aggregates and articulates a heterogeneous group of national and European actors for necessary cooperation at each level in case of major cyber incident.
4. It is very important that the recommendations set out by the Blueprint for a joint response to large-scale cyber incidents and crises fit into the current EU crisis management systems.
5. Throughout the incident or crisis, lower levels of cooperation will alert, inform and support the higher levels; the higher levels will provide guidance and decisions to the lower levels, as appropriate.
6. In particular, at strategic/political level Blueprint is mainly channel through the Integrated Political Crisis Response, where the complexity and divergence of relevant national political bodies is simplified by working through a national contact point, who streams the contacts and communications from and towards the EU institutions.
7. There is an important gap on how these three levels (Technical (CSIRT Network), Operational (Cyclone) and Strategical/Political (IPCR/Cyber Diplomacy/...).) are connected and the procedures to work together.
8. On the other hand, it is important to highlight that it should be taken into account the fact that these mechanisms must be adapted according to the target groups: SME, essential operator, public sector, etc.
9. Regarding public communication, it must be noticed that it is paramount to align announcements, and published them through official means.
10. Not only a bottom-up approach is needed, but also the same reflection is required from top to bottom, in order to established proper channels of communication. This mechanism should be also set up at European level, supported by this Joint Cybersecurity Unit.
11. As regards information sharing, it is necessary to follow a bottom-up approach, from technical level to operational in each Member State, and finally to the political level. It is very important to have sharing, escalating and mitigation procedures in place, taking into account interoperability and the means to export information through secure channels.
12. The development of common and aggregated evaluation mechanisms would lead to a more particular vision of the cybersecurity situation at European level. This would have to be done at many levels as above explained, and according to specific themes in order to combine improvement, support and capacity building actions.
13. Regarding cybercrime, it is essential to guarantee that the technical and operational information handled by the existing groups named in the recommendation -such as the CSIRT Network of the NIS ecosystem or the INTCEN- is channelled, in a systematic way, to the Law Enforcement Agencies with a view to the persecution of cybercrime (it does not happened nowadays). In order to alleviate these deficiencies, it would be advisable to integrate the information generated by all the JCU participants on cybersecurity matters at the European level. This could be done through the creation and empowerment of a common cyber intelligence database or tool on the virtual platform referred to in this recommendation. This tool would allow the agile exchange

of Indicators of Compromise, as well as Technical Tactics and Procedures used in attacks. Initiatives such as MISP or OpenCTI can be a basis for this. This collaboration or contribution in the matter of criminal prosecution of cyberattacks should be articulated through the mechanisms contemplated in Directive 2013/40.

14. The Joint Cyber Unit should focus on these areas and topics that are no cover yet, but avoiding duplicating efforts and respecting competences and responsibilities of CERTS from Defense and Civilian Organizations in the appropriate networks. The development of common and aggregated evaluation mechanisms would lead to a more particular vision of the cybersecurity situation at European level. This would have to be done at many levels as above explained, and according to specific themes in order to combine improvement, support and capacity building actions.
15. The integration of cooperation mechanisms in case of crisis through the JCU seems appropriate in order to avoid duplication and improve the efficiency and effectiveness in the exchange of information.
16. The integration of civil society capacities in this unit is considered essential, and its presence in the final phase of the gradual process of creating the JCU is valued as adequate. However, the mechanisms for collaboration and sharing of public-private information should be compartmentalized in the JCU to avoid the presence of commercial interests on the part of private entities.
17. Member States should be full members at the Joint Cyber Unit, where public and private sector should be integrated, and specially, official organisms that support industry, research and development.

Conclusions

1. Spain welcomes the JCU proposal.
2. The JCU must avoid creating duplications in both structures and procedures. It should focus on filling the existing gaps and improving the collaboration of all actors.
3. The JCU must add value to the current cyber ecosystem and concretely to the development of Blueprint.
4. Due to the JCU will be based on cooperation of all actors under a memoranda of understanding, a legal assessment should be carried out in order to clarify the legal capacity of different actors within the JCU roles and especially, in mutual assistance mechanisms.
5. The JCU implementation and integration with existing frameworks and capacities, should be funded under the EU financing programmes, primarily the Digital Europe Programme.
6. The EMMs must take part in the development, implementation and decision-making process.
7. The EMMs must be full members at the Joint Cyber Unit, where public and private sector should be integrated.
8. The JCU project must have political support through the Council. The initiative for the Council to draw conclusions that may qualify the Recommendation and study the initiative and its implementation in greater depth is supported.