MPR PARTNERS

THE EU COMMISSION PRESENTS NEXT STEPS IN THE SETTING UP OF THE JOINT CYBER UNIT

1. Background of the proposed changes

The COVID-19 pandemic has boosted digitalization and digital interaction at all levels of European society. Along with increased interconnectivity, however, came greater vulnerabilities and threats from a cybersecurity perspective.

In order to deliver seamless public digital services, the European Union ("**EU**") focuses on increasing its cybersecurity capabilities, by implementing a series of measures announced in the EU's Cybersecurity Strategy for the Digital Decade, communicated on December 16, 2020.

According to the Strategy, the European Commission ("**Commission**") has been tasked with coordinating and implementing the setting-up of a new Joint Cyber Unit. The Joint Cyber Unit should become the infrastructure for increased cooperation between Member States and all the relevant EU cybersecurity institutions, bodies, and agencies, and for the full development of existing networks and communities with respect to information sharing, including with the private sector.

Further steps in this regard have been presented in the Commission's Recommendation on the creation of the Joint Cyber Unit issued on June 23.

2. Cyber Joint Unit attributions

The Joint Cyber Unit is meant to function as a common EU platform for safe and efficient exchange of information among different cybersecurity communities and coordination and mobilisation of operational capabilities by relevant actors.

The Commission stresses that the Joint Cyber Unit would not be an additional, standalone body or affect the role and functions of existing authorities, but it would help bring them together and tap into each other's expertise. The creation of the Joint Cyber Unit would rest on memoranda of understanding among the participants to the platform. Such participants should come from all cybersecurity communities, i.e., civilian, law enforcement, diplomacy, and defence.

The Joint Cyber Unit will have both a physical and a virtual presence. Its role is to bring together technical and operational crisis management experts from Member States and EU entities, in order to coordinate responses to cyber threats. The Commission hopes that the experts participating in the Joint Cyber Unit will be able to monitor and protect a much wider attack surface by making use of both the physical and virtual platform, especially in cross-border incidents.

3. Steps for setting-up the Joint Cyber Unit

The Commission aims for the Joint Cyber Unit to be operational by June 30, 2022. There are four main steps to be followed:

(i) assessment phase – by December 31, 2021, the Joint Cyber Unit's organisational aspects and operational capabilities must be identified;

(ii) planning phase – by June 30, 2022, the EU Cybersecurity Incident and Crisis Response Plan must be prepared, based on national cybersecurity incident and crisis response plans prepared by Member States, which should define objectives and modalities in the management of large-scale cybersecurity incidents and crises;

(iii) operational phase – by December 31, 2022, the Joint Cyber Unit should be operational and ready to carry out technical and operational activities; and

(iv) cooperation expansion phase – by June 30, 2023, participants to the Joint Cyber Unit submit a progress report; also, they must share information with the private sector and provide incident response services to the private sector.

Financing for the creation of the physical and virtual platform of the Joint Cyber Unit and for creating and maintaining communication channels and improving detection capabilities will be ensured by the Commission mainly through the Digital Europe Programme.

4. Conclusions

Creating the Joint Cyber Unit is deemed by the Commission as an important step towards completing the European cybersecurity crisis management framework, within the EU Cybersecurity Strategy and the EU Security Union Strategy.

Cybersecurity remains a top priority for the Commission, given the increase of cyberattacks during the COVID-19 pandemic, which has shown the importance of vulnerabilities in critical infrastructure.

*****

This article contains general information and should not be considered as legal advice.

Senior Associate

flavia.stefura@mprpartners.com

Senior Privacy & Technology Consultant

cristina.cretu@mprpartners.com