Commission Recommends Joint Cyber Unit

Anna Pingen

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Anna Pingen
Researcher
Max Planck Institute for the Study of Crime, Security and Law

ISSN: 1862-6947
https://eucrim.eu

On 23 June 20201, the Commission presented a recommendation on building a Joint Cyber Unit. Acccording to the Commission, the pandemic has increased the importance of connectivity and shown how important reliable and secure networks/information systems are, especially for entities in the frontline of the fight against the pandemic (e.g., hospitals and vaccine manufacturers). In order to face these challenges and prevent the loss of lives, the Commission voiced the need for a coordinated EU effort to prevent, detect, and respond to the most impactful cyber-attacks. Improved coordination between relevant cybersecurity institutions and relevant actors in the EU should also help address the cross-border nature of cybersecurity threats and the steady surge of more complex, pervasive, and targeted attacks.

Despite major progress in achieving cybersecurity – i.e., through cooperation between Member States and relevant EU institutions, bodies, and agencies (EUIs) and by means of the existing legislative framework – there is still no common EU platform where information gathered in different cybersecurity communities can be exchanged. In addition, a mechanism does not yet exist for harnessing existing resources, providing mutual assistance across the cyber communities, combating cybercrime, and conducting cyber-diplomacy.

In order to fill this gap and coordinate the EU effort against cyber-threats, incidents, and crises, the Commission has developed a concept for a Joint Cyber Unit that will offer coordinated assistance to Member States and EUIs in times of crisis. The platform (which will exist in both a virtual and a physical format) will involve the expertise of civilian, law enforcement, diplomatic, and cyber defence communities. The Joint Cyber Unit will identify technical and operational capabilities, experts, and equipment ready to be deployed to Member States. It is designed to provide a new impulse to European cybersecurity crisis management by ensuring a coordinated EU response. Participants in the Joint Cyber Unit should be able to engage with a wider range of stakeholders and simultaneously benefit from enhanced preparedness and greater situational awareness, covering all aspects of cybersecurity threats. Through the Unit, participants should also be able to integrate private sector stakeholders, including both providers and users of cybersecurity solutions and services.

For the purpose of establishing the Joint Cyber Unit, the Commission proposed a gradual and transparent process to be completed over the next two years. In the Annex to its Recommendation, the Commission further proposed that the objectives set out in the Recommendation be achieved in a four-step process:

Step 4: Expanding cooperation within the Joint Cyber Unit to private entities and reporting on progress made. Step four should be fully completed by 30 June 2023.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by the European Union