Council Conclusions on Cybersecurity Strategy

Thomas Wahl

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Thomas Wahl
Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

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

On 22 March 2021, the Council adopted conclusions on the EU's cybersecurity strategy. The new cybersecurity strategy for the digital decade was jointly presented by the Commission and the High Representative for Foreign Affairs and Security Policy in December 2020 (→ eucrim 4/2020, 282). It provides a framework for EU action to protect citizens and businesses from cyber threats, promote secure information systems, and protect a global, open, free, and secure cyberspace.

The Council stressed that cybersecurity is essential for building a resilient, green, and digital Europe. In particular, it is about achieving strategic autonomy to strengthen the EU's digital leadership.

The conclusions highlight a number of areas for action in the coming years, e.g.:

- Regular and structured exchanges with multiple stakeholders, including the private sector, academia, and civil society organisations;
- Swift establishment and implementation of the European network of cybersecurity centres;
- Creation of security operation centres in the EU Member States, which are enabled to further monitor and anticipate signals of attacks on networks;
- Definition of a joint cyber unit that would contribute to the EU's cybersecurity crisis management;
- Engagement in the development of international cybersecurity standards as well as the EU's cybersecurity certification schemes;
- Swift completion of the EU's 5G toolbox with measures that guarantee the security of 5G networks;
- Enhancement of international cooperation to combat cybercrime, including the exchange of best practices and technical knowledge and support for capacity building;
- Possible establishment of a Member States' cyber intelligence working group in order to strengthen the EU Intelligence Analysis Centre's (EU-INTCEN's) work as a hub for situational awareness and threat assessments on cyber issues;
- Increasing the effectiveness and the efficiency of the cyber diplomacy toolbox, which should devote special attention to preventing and countering cyberattacks having systemic effects;
- Strengthened cooperation with international organisations and partner countries in order to advance the shared understanding of the cyber threat landscape.

As regards law enforcement cooperation, the conclusions stress the need to improve the capacity of law enforcement and judicial authorities to investigate and prosecute cybercrime. This must include facilitated cross-border access to electronic evidence, which must respect due process and other safeguards. The Council also reaffirms its support for the development, implementation, and use of strong encryption as a necessary means of protecting fundamental rights and the digital security of individuals, businesses, and

governments. At the same time, the competent authorities in the areas of security and criminal justice must be able to obtain access to data in a lawful and targeted manner.

Next steps: The Council encourages the Commission and the High Representative to establish a detailed implementation plan in order to ensure the development, implementation, and monitoring of proposals presented under the Cyber Security Strategy. The Council will monitor progress in implementing the conclusions through an action plan.

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