Council Conclusions on the Future of Cybersecurity

Anna Pingen

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

On 21 May 2024, the Council adopted a comprehensive set of conclusions aimed at strengthening cybersecurity across the EU, underlining the need for a more resilient and secure digital landscape. Recognizing the increasing scale, complexity, and frequency of cyber threats, exacerbated by global geopolitical tensions, the Council stressed the critical importance of cybersecurity for the functioning of modern society and the economy. The conclusions outline the future direction for EU cybersecurity, focusing on several key areas:

- **Implementation and harmonisation**: The Council emphasises the need for effective implementation of existing cybersecurity frameworks, in particular newly established rules such as the Directive on Network and Information Security (NIS II) and the Cyber Resilience Act. Harmonised standards and certifications are highlighted as crucial to reducing administrative burdens and ensuring consistent security measures across Member States. The Council cautions against the fragmentation of cybersecurity rules across different sectors and calls for a coherent and unified approach to cybersecurity policy.
- **Support for SMEs and innovation**: Small and medium-sized enterprises (SMEs) often lack the resources to implement robust cybersecurity measures. The Council calls for measures to facilitate compliance, reduce administrative burdens, and provide practical guidance to help SMEs improve their cybersecurity standing. In addition, the Commission and relevant bodies are urged to stimulate investment in cybersecurity research and development, in particular through the European Cybersecurity Competence Centre (ECCC).
- **International cooperation**: The Council underscores the importance of international cybersecurity cooperation, in particular with third countries and international organisations such as NATO, the UN, and the Organisation for Security and Co-operation in Europe (OSCE). It points out the need for a strong external cybersecurity policy to complement internal efforts and emphasises the importance of transatlantic cooperation and initiatives such as the EU-US Joint Cyber Safe Product Action Plan. The Council also calls for increased engagement with countries outside the EU to combat cybercrime and improve global cyber resilience.
- **Addressing emerging threats**: The conclusions acknowledge the potential benefits that technologies such as artificial intelligence (AI), quantum computing, and 6G technology could bring to cybersecurity. But they also recognise the challenges posed by such emerging and potentially disruptive technologies, namely the need for careful risk management and the development of concrete initiatives to address these new threats. The transition to Post-Quantum Cryptography (PQC) is identified as a priority in order to protect sensitive information from future quantum threats.

AUTHOR

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

Published in
2024, Vol. 19(2) eucrim
ISSN: 1862-6947
https://eucrim.eu

- **Strengthening institutional frameworks**: EU cybersecurity institutions, such as the European Union Agency for Cybersecurity (ENISA), the ECCC, and the network of Computer Emergency Response Teams (CERTs) should be further strengthened. Reforms should include a clear delineation of roles and responsibilities between these bodies to avoid duplication and ensure effective coordination. The importance of sufficient funding and skilled cybersecurity experts to support these institutions is also emphasised.
- **Cybersecurity crisis management**: The conclusions address the need for a robust cybersecurity crisis management framework, building on existing structures and ensuring seamless coordination across sectors and borders. The Commission is invited to propose a revised Cybersecurity Blueprint that takes into account the current complex threat landscape, enhances cooperation, and breaks down silos between organisations.
- **Private sector engagement**: Recognising the key role of the private sector in securing digital infrastructure, the Council calls for greater cooperation between public authorities and private companies. This includes promoting information sharing, supporting SMEs, and developing joint initiatives to mitigate cyber threats.

The Council's conclusions that include important cybersecurity principles will be the basic framework for future action with the aim of strengthening the EU's collective ability to protect, detect, and respond to cyber threats/attacks. The Council invited the European Commission and the High Representative to review and update the 2020 EU Cybersecurity Strategy to ensure that it remains fit for purpose in light of the evolving threat landscape.

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