ECA Dissatisfied with EU's Cybersecurity Performance

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

Multiple challenges exist to strengthen EU's cybersecurity and its digital autonomy, and the EU needs to do more. This is the main outcome of a briefing paper by the European Court of Auditors (ECA) that was published on 19 March 2019.

The briefing paper provides an overview of the EU's cybersecurity policy landscape and identifies major challenges to effective policy delivery. It covers network and information security, cybercrime, cyber defence, and disinformation. The majority of research was carried out between April and September 2018; developments up to December 2018 were taken into account.

The challenges are grouped into four clusters:

- The policy framework;
- Funding and spending;
- Building cyber-resilience;
- Responding effectively to cyber incidents.

Each chapter ends with reflection points that are addressed to policymakers, legislators, and practitioners.

The authors of the briefing paper conclude that the EU's ambition to become the world's safest digital environment is a monumental task. In order to achieve accountability, the EU needs to shift towards a performance culture with embedded evaluation practices.

Gaps remain in existing legislation that is not being consistently transposed by the EU Member States. As a result, legislation cannot reach its full potential.

Another significant challenge is to overcome fragmented spending in the cybersecurity research field. There is no clear picture of funding and spending. Investments must be aligned with strategic goals. The paper also addresses constraints in the adequate resourcing of the EU's relevant cybersecurity agencies which entails difficulties in attracting and retaining talents.

As regards building cyber-resilience, the ECA notes that there is a global weakness in cybersecurity governance, which impairs the global community's ability to respond to and prevent cyberattacks. Governance issues also impede the EU's aim to take a coherent approach. The ECA recommends improving skills and awareness across all sectors in order to overcome the growing global skills shortfall. This must be flanked by better information exchange and coordination between the public and private sectors.

For an effective response to cyber-attacks, key challenges for the EU remain rapid detection and response as well as protection of critical infrastructure and societal functions. In the latter context, further challenges are posed by potential interference in electoral processes and disinformation campaigns, especially in view of European Parliament elections.

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