Planned revision of the Cyber Security Act

Response to the Commission´s call for evidence for the revision of the Cybersecurity Act, intended to clarify the mandate of the EU Agency for Cybersecurity (ENISA) and improve the European Cybersecurity Certification Framework to achieve better resilience[1].

18th of June 2025

epicenter.works welcomes the European Commission's initiative to revise the Cybersecurity Act. Cybersecurity is not merely a technical issue. It is a core pillar of democratic resilience, fundamental rights, and inclusive digitalisation. From our perspective, three key priorities must be at the heart of this revision:

1. Strengthening regulatory foundations to enable secure digitalisation

The recurring narrative that Europe is stifling innovation and burdening businesses through over regulation of digital policy fields is misleading. Regulation is too often made the scapegoat for deeper policy failures: missed opportunities in strategic funding[2], ineffective public procurement, a widening digital skills gap[3], and a lack of political vision. Blaming cybersecurity rules is an easier and faster "win" for politicians than addressing these structural challenges, which are harder to solve and often more costly.

In cybersecurity, well-crafted regulation is not a burden. It is a prerequisite for a secure and functional digital society. The benefits of digitalisation such as a more inclusive and connected society, innovation, and economic efficiency can only be realised if people trust the technologies they rely on. That trust depends on the perception that data, infrastructure, and communications are protected from misuse, manipulation, and attacks.

These risks are not theoretical. Citizens are already experiencing the downsides of insecure digitalisation: ransomware attacks on critical infrastructure, phishing campaigns targeting vulnerable populations, and severe vulnerabilities in everyday digital services. In the face of such real and growing threats, the appropriate policy response cannot be to „simplify". It must be to regulate smartly, ensuring security and resilience.

Good regulation in this context does not mean bureaucracy. It means protection through clear responsibilities, enforceable standards, and stable mechanisms for reducing systemic risk. Properly designed, regulation enables innovation by creating clarity, reducing uncertainty, and fostering public trust.

2. Expanding ENISA's mandate and operational capabilities

The cybersecurity landscape is evolving rapidly: technologically, geopolitically, and societally. If the EU intends to keep pace, it must strengthen its institutional capacity. ENISA already plays a crucial role in this regard. Often, its European outlook and technical approach prove more balanced than that of certain national authorities, which can be shaped by narrow domestic agendas.
But ENISA's current mandate and resources are insufficient to meet the moment. Effective cybersecurity coordination at EU level requires a mandate strong enough to overcome national

1 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14578-The-EU-Cybersecurity-Act_en
2 https://www.eib.org/en/publications/20220206-european-cybersecurity-investment-platform
3 https://www.enisa.europa.eu/news/skills-shortage-and-unpatched-systems-soar-to-high-ranking-2030-cyber-threats

fragmentation. Only through meaningful cooperation among Member States can we achieve the critical mass of expertise needed to secure our digital ecosystem.

ENISA must also be empowered to prevent delays in the development and adoption of cybersecurity standards. Delays that too often result from intergovernmental deadlock. A more empowered role for ENISA can ensure the consistent application of standards across the Single Market, safeguard against regulatory arbitrage, and promote legal certainty for economic actors. If the EU takes „digital sovereignty" seriously, it must give ENISA the independence, budget, and staff it needs to lead.

3. Integrating civil society and academia into cybersecurity governance

Cybersecurity is no longer the exclusive domain of states. Yet many European governments still operate with a state-centric mindset. They prioritise control over resilience and sideline key actors in the process. This model is no longer fit for purpose. Modern cyber threats demand decentralised responses, interdisciplinary cooperation, and proactive engagement with civil society.
Europe is facing a major shortage of cybersecurity professionals. And yet, instead of embracing all available expertise, many governments actively push valuable contributors away. One stark example is the criminalisation of ethical hackers and security researchers. Those who responsibly disclose vulnerabilities have faced prosecution, as in the case of a German researcher who identified a serious flaw in a political party's campaign app[4]. Instead of being thanked, she was reported to law enforcement. This sends a chilling message: even good-faith actions can lead to punishment, ultimately weakening security for everyone.

At the same time, civil society and academia are often excluded from national cybersecurity policy-making. Austria's strategy, for instance, is drafted solely by state agencies, without formal consultation of external experts. This reflects outdated thinking and ignores the reality that cybersecurity expertise is distributed across sectors.

Other EU countries are setting better examples. The Netherlands has introduced a legal framework for responsible vulnerability disclosure that protects researchers and strengthens trust[5]. Italy has established a scientific advisory board that brings technical experts into national decision-making[6]. These models show that cybersecurity policy is most effective when informed by real-world experience, not only political interests.

The revision should establish structured, ongoing mechanisms for engaging civil society and academic experts in EU cybersecurity decision-making, including legal protections for ethical hackers and transparent consultation frameworks.

Sincerely,

epicenter.works – for digital rights

4 https://netzpolitik.org/2021/cdu-connect-ermittlungsverfahren-gegen-sicherheitsforscherin-lilith-wittmann-eingestellt/
5 https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
6 https://www.acn.gov.it/portale/en/comitato-tecnico-scientifico