



Press Release

Luxembourg, 19 March 2019

Multiple challenges in EU cybersecurity, warn auditors

Multiple challenges in strengthening EU cybersecurity remain despite the progress made, according to a new Briefing Paper from the European Court of Auditors. As the risk of falling victim to cybercrime or a cyberattack increases, it is essential to build resilience through strengthening governance, raising skills and awareness, and improving coordination, say the auditors. They also highlight the importance of meaningful accountability and evaluation to help the EU achieve its aim of becoming the world's safest digital environment.

The Briefing Paper aims to provide an overview of the EU's cybersecurity policy landscape, which the authors describe as complex and uneven, and to identify the main challenges to effective policy delivery.

"The current challenges posed by cyber threats make this a critical time for the EU to strengthen its cybersecurity and its digital autonomy, while requiring continued commitment to the EU's core values," said **Baudilio Tomé Muguruza, the member of the European Court of Auditors responsible for the Briefing Paper.**

The auditors consider the challenges facing cyber policy under four main headings: the policy and legislative framework; funding and spending; building cyber-resilience; and responding effectively to cyber incidents.

The policy and legislative framework: the EU's cyber ecosystem is complex and multi-layered. Trying to forge all of these moving parts together into a comprehensive, strategic, coherent and coordinated way is a key challenge. Developing action aligned to EU cybersecurity strategy is a challenge in the absence of measurable objectives and scarce, reliable data. Outcomes are rarely measured and few policy areas have been evaluated, including the state of EU cybersecurity and readiness. The challenge is therefore to shift towards a performance culture with embedded evaluation practices.

Funding and spending: spending in the EU on cybersecurity has been low and fragmented, according to the paper. The EU and its Member States need to know how much is being invested collectively to know which gaps to close, but forming a clear picture of this is difficult. There is no

The purpose of this press release is to give the main messages of the briefing paper by the European Court of Auditors. The full paper is on www.eca.europa.eu.

ECA Press

Mark Rogerson – Spokesperson T: (+352) 4398 47063

Damijan Fišer – Press Officer T: (+352) 4398 45410

12, rue Alcide De Gasperi - L-1615 Luxembourg

E: press@eca.europa.eu @EUAuditors eca.europa.eu

M: (+352) 691 55 30 63

M: (+352) 621 55 22 24

dedicated EU budget to fund the cybersecurity strategy or a clear picture of what money goes where.

The Commission is working to overcome fragmentation in the cybersecurity research field, but to date results from investment in research are often not well patented, commercialised or scaled up, holding back the EU's resilience, competitiveness and its autonomy.

Building cyber-resilience: the absence of a coherent, international cybersecurity governance framework impairs the global community's ability to respond to and prevent cyberattacks. Weaknesses in cybersecurity governance abound in the public and private sectors across the EU. This poses a challenge to a coherent EU-wide approach to cybersecurity. In addition, given the growing global cybersecurity skills shortfall, raising skills and awareness across all sectors and levels of society is essential.

Responding effectively to cyber-incidents: digital systems have become so complex that preventing every attack is impossible. The challenge is therefore rapid detection and response. Cybersecurity is not yet fully integrated into existing EU-level crisis response coordination mechanisms, potentially limiting the Union's capacity to respond to large-scale, cross-border cyber incidents. The potential interference in electoral processes and disinformation campaigns are also a critical challenge, especially in view of the European Parliamentary elections in May 2019.

Notes to Editors

A Briefing Paper is a descriptive and analytical document concerning a policy area. It does not contain audit findings. The analysis in this paper is based on a documentary review of publicly available information in official documents, position papers and third party studies. Field work was carried out between April and September 2018, and developments up to December 2018 are taken into account. The auditors complemented their work with a survey of Member States' national audit offices, and through interviews with key stakeholders from EU institutions and representatives from the private sector.

The ECA's briefing paper "Challenges to effective EU cybersecurity policy" is available on the ECA website (eca.europa.eu) in 23 EU languages.