Resolution on the EU’s Cybersecurity Strategy for the Digital Decade

2021/2568(RSP) - 10/06/2021 - Text adopted by Parliament, single reading

The European Parliament adopted by 670 votes to 4, with 12 abstentions, a resolution on the EU’s Cybersecurity Strategy for the Digital Decade.

Parliament recalled that digital transformation - a key strategic priority for the EU - is inevitably associated with increased exposure to cyber threats.

The COVID-19 crisis has exacerbated cyber vulnerabilities in some critical sectors, in particular healthcare, while teleworking measures have increased dependence on digital technologies.

The number of cyber-attacks is increasing dramatically and hybrid threats, which include the use of disinformation campaigns and cyber-attacks against infrastructure, economic processes and democratic institutions, are growing in number and concern.

Secure and resilient connected products against cyber threats

Members called for a goal to be set to ensure that all internet-connected products available in the EU, as well as the entire supply chains that make them available, are secure by design, resilient to cyber incidents and updated as soon as possible when vulnerabilities are discovered.

Parliament welcomed the Commission's intention to **propose horizontal legislation** on cybersecurity requirements for connected products and associated services. It called for such legislation to provide for harmonisation of national laws to avoid fragmentation of the single market. It also invited the Commission to assess the need for a proposal for a horizontal regulation introducing cyber security requirements for applications, software, embedded software and operating systems by 2023.

Cybersecurity policies

Stressing the need to integrate cybersecurity into digitisation, Parliament called for EU-funded digitisation projects to include **cybersecurity requirements**. It welcomed support for research and innovation, especially in disruptive technologies (such as quantum computing and quantum cryptography) and called for further research into post-quantum algorithms as a standard for cyber security.

Parliament insisted that cybersecurity policies should be integrated into the EU's digital strategy and its funding, and that they should be coherent and interoperable across sectors. It recommended a coherent use of EU funds for cyber security.

Critical infrastructure

Parliament stressed the need for a **new robust security framework** for the EU's critical infrastructure to safeguard the EU's security interests and to build on existing capabilities to respond appropriately to risks, threats and technological changes.

Members called on the Commission to develop provisions to **ensure the accessibility, availability and integrity of the public core of the internet** and thus the stability of cyberspace. They welcomed the EU's 5G cybersecurity toolkit and called on the Commission, Member States and industry to continue their efforts to promote secure communication networks.

Strategic resilience of the EU

The Commission and the Member States are invited to **pool their resources** in order to strengthen the EU's strategic resilience, reduce its dependence on foreign technologies and promote its leadership and competitiveness in cybersecurity across the digital supply chain, including cloud data storage and processing, processor technologies, integrated circuits (chips), ultra-secure connectivity, quantum computing and next-generation networks.

The resolution stressed the need for a strong and coherent security framework to protect all EU personnel, data, communication networks and information systems, as well as decision-making processes, against cyber threats, and the importance of basing this framework on comprehensive, coherent and consistent rules and appropriate governance.

Members called on the Commission and Member States to build confidence and reduce barriers to sharing information on cyber threats and attacks at all levels.