Recent cyber-attacks and the EU's cybersecurity strategy for the digital decade

Increasing digitalisation means that public administration at EU and national levels has come to rely on digital technologies as a means of carrying out their core functions, a process that has been intensified by the pandemic. This growing reliance on digital technologies, while beneficial, has also increased the risk of cyber-attacks, and key institutions at EU and national level have recently been targeted by cyber-attacks. During the June I plenary session, Members of the European Parliament will debate with the Council and the Commission on recent cyber-attacks in the EU, and discuss the European Union's cybersecurity strategy for the digital decade.

Background

The rapidly progressing digitalisation of the economy and society has created new opportunities for cyber-attacks. Key sectors such as health, finance, energy and telecommunications rely on network and information systems that are increasingly interconnected. Changes in working patterns have been accelerated by the coronavirus pandemic, with 40 % of EU workers switching to remote working in early 2020. These changes have provided increased opportunities for cybercrime, including attacks on critical infrastructure.

Recent cyber-attacks on EU institutions and at national level

The EU's cybersecurity agency ENISA has reported the detection of 230 000 new malware infections every day during the period from January 2019 to April 2020, while Europol's 2021 Serious and Organised Crime Threat Assessment has highlighted a 'notable' increase in the number of ransomware attacks on public institutions and large companies. Its Internet Organised Crime Threat Assessment states that targeting such entities allows threat actors to increase the ransom amount requested and notes attacks on local governments and ministries, as well as other public sector organisations in healthcare and education, and businesses in manufacturing, finance, energy and transport. These cyber-attacks have targeted EU institutions and bodies, as well as Member States' critical infrastructure.

Media sources have reported a recent 'significant' cyber-attack on a range of EU institutions, including the European Commission, while the European Medicines Agency and the European Banking Authority have both confirmed that they were subject to cyber-attacks. At Member State level, in May 2021 Ireland's health service fell victim to a 'catastrophic' ransomware attack, which led to a shutdown of its ICT system, with widespread cancellation of patient services. In the same month in Belgium there were two large scale cyber-attacks against public service organisations. The first concerned Belnet, the network which serves third-level institutions and research centres, as well as hospitals and federal ministries. The Internal Affairs Department, the federal ministry responsible for the rule of law, immigration policy and public order, was subjected to a cyber-attack of such a scale that it has raised suspicions of the involvement of a foreign state.

The EU's cybersecurity strategy for the digital decade

The EU's cybersecurity policy provides the EU and its Member States with strong tools to ensure the security of critical infrastructure and institutions at EU and national level. In December 2020, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy published a joint communication on the EU's cybersecurity strategy for the digital decade. The strategy aims to bolster Europe's collective resilience against cyber-threats, and ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. Following on from the strategy, the Commission adopted two proposals in December 2020: a proposal for a directive on measures for high common level of cybersecurity across the Union ('revised NIS directive' or 'NIS 2') and a proposal for a new directive on the resilience of critical entities. NIS 2 aims to strengthen EU cybersecurity capabilities, with proposals for information sharing and cooperation on cyber-crisis management at national and EU

Author: Ann Neville, Members' Research Service
PE 690.639 – June 2021

level, while the directive on the resilience of critical entities provides for an all-hazards framework to support Member States in ensuring that critical entities are able to prevent, resist and recover from disruptive incidents whatever their source.

In March 2021, the Council adopted conclusions on the cybersecurity strategy, highlighting a number of areas for action in the coming years, including the design of a network of security operational centres (SOCs) across the EU to monitor and anticipate signals of attacks on networks, and the common cyber unit to provide clear focus to the EU's cybersecurity crisis management framework. It also focuses on the finalisation of the EU 5G toolbox and the establishment of key internet security standards. It supports the development of strong encryption, while also permitting law enforcement and judicial authorities to exercise their powers both online and offline, and strengthens the cyber-diplomacy toolbox with a view to preventing and countering cyber-attacks with systemic effects.

European Parliament position

During the June I plenary session, the Parliament will hear Council and Commission statements addressing issues arising from recent cyber-attacks on EU institutions and on sensitive national public and private institutions in various Member States. While welcoming the recent EU cybersecurity strategy for the digital decade, the oral question asked of the Commission by the Committee on Industry, Research and Energy, seeks information on how the Commission will ensure connected devices can all be made 'secure by design', and resilient to cyber-attacks. In addition, the question asks how EU autonomy in the area of cybersecurity can be strengthened, and how even with increased cybersecurity the internet can be kept 'free, open and neutral'.

Oral question: O-000037/2021. Committee responsible: ITRE. For further information see the EP Legislative Train Schedule on the cybersecurity package, the review of the Directive on Security of Network and information Systems and the resilience of critical entities.