

Cyber security: Member states should cooperate with strategic partners

Damaging cyberattacks can take place at any time, and European and member state actors should be encouraged to take all necessary measures, say MEPs.

The continuous increase in recent years of malicious cyber operations against the EU and its Member States have revealed vulnerabilities in networks essential to European security, MEPs have warned in a report adopted by the Foreign Affairs Committee on Thursday.

These operations are conducted by state and non-state actors and are growing in diversity, sophistication and frequency. Because of these attacks, it is a matter of priority to step up defence capacity and develop cyber European capabilities, the report says.

MEPs say damaging cyberattacks can take place at any moment and actors on both the European and national level should be encouraged to take the necessary measures to maintain effective cyber defence capabilities during peacetime.

According to the report, cyber defence refers to actions, instruments and processes, which are proportionate and in line with international law, and which includes military and civilian elements.

The EU's ability to develop cyber defence projects depends on the control of technologies, equipment, services, data and data processing and has to rely on a trusted sectoral stakeholder base, say MEPs. They call on member states to take advantage of the [European Defence Fund \(EDF\)](#) to jointly develop cyber defence capabilities.

MEPs also stress that private companies mainly drive technological innovation, and therefore cooperation with the private sector and civilian stakeholders, including industries, SMEs or civil society, is crucial and should be reinforced.

Rapporteur [Urmass Paet \(Renew, Estonia\)](#) said: "In recent years, we've clearly seen a growth in cyber operations conducted by state and non-state actors. In order to tackle these threats we need closer cooperation on cyber defence between member states, the EU institutions, NATO, the United States and other strategic partners. Furthermore, raising the EU's level of cyber security is of key importance to the success of our digital ambitions".

The report was adopted by 58 votes in favour, 7 votes against and 3 abstentions.

Next steps

The report will now be submitted to a vote in the European Parliament as a whole after the upcoming summer recess.

Further information

[Report will be available here](#)

[Procedure file](#)

[EPRS Briefing: The new European cybersecurity competence centre and network, 19.05.2021](#)

[EPRS Briefing: Understanding the EU's approach to cyber diplomacy and cyber defence, 28.05.2020](#)

[Subcommittee on Security and Defence](#)

[Committee on Foreign Affairs](#)

Contacts

Snježana KOBESČAK SMODIŠ

Press Officer

☎ (+32) 2 28 32547 (BXL)

☎ (+33) 3 881 74007 (STR)

📱 (+32) 470 96 08 19

✉ snjezana.kobescak@europarl.europa.eu
