
Cyber defence: MEPs call for better European cooperation

- Better prevention and response to cyber attacks
- Use EU-NATO cooperation and Military Erasmus Programme
- Set up European cyber rapid response team

The EU member states should work together closely on cyber defence, following increasing cyber-attacks on civilians and military targets, said MEPs on Wednesday.

The resolution notes that different states, such as Russia, China and North Korea, but also non-state actors, have carried out malicious cyber activities and attacks on critical infrastructure, cyber-espionage, mass surveillance of EU citizens, disinformation campaigns and have limited access to the internet (such as Wannacry, NonPetya).

More cyber cooperation

Foreign affairs and defence MEPs stress that fragmented European defence strategies and capabilities have led to the current vulnerability to cyber-attacks. Therefore, they urge member states to enhance the ability of their armed forces to work together and to strengthen cyber cooperation at European level, with NATO and other partners through situational awareness, cyber exercises, Military Erasmus (an exchange programme between member states for future military officers, their teachers and instructors) and other joint training and exchange initiatives.

Given the permanent shortage of highly qualified cyber defence specialists, in particular experts in cyber forensics, MEPs call on member states to invest more in this field and facilitate cooperation between civil academic institutions and military academies, supporting the field of cyber defence education. They also call on the European External Action Service (EEAS), and on member states which provide the headquarters for Common Security and Defence Policy

(CSDP) operations, to strengthen the cyber defence expertise of the EU's missions and operations.

European cyber rapid response team

MEPs welcome two cyber projects to be launched within the [Permanent Structured Cooperation \(PESCO\)](#), namely an information-sharing platform for cyber incidents and cyber rapid response teams. They hope it will lead to the creation of a European cyber rapid response team, which would coordinate, detect and counter collective cyber threats.

Quote

Parliament's rapporteur [Urmás Paet \(ALDE, EE\)](#) said: "Cyber defence remains a core competence of the member states, but due to the borderless nature of cyberspace, it is not possible for any one state to tackle the threats and challenges alone. The EU needs to strengthen its cyber defence capabilities by boosting cooperation between member states, the EU and NATO. We also need to train more experts in cyber defence and organise joint exercises."

Next steps

The resolution on cyber defence was approved by 45 votes to 8, with 8 abstentions. The full House is to vote on it at the June plenary session in Strasbourg.

Procedure: Non-legislative resolution

Further information

[Committee on Foreign Affairs](#)
[Subcommittee on Security and Defence](#)
[EP rapporteur Urmás PAET \(ALDE, EE\)](#)
[Procedure file](#)

Contacts

Gediminas VILKAS

Press Officer

 (+32) 2 28 46396 (BXL)

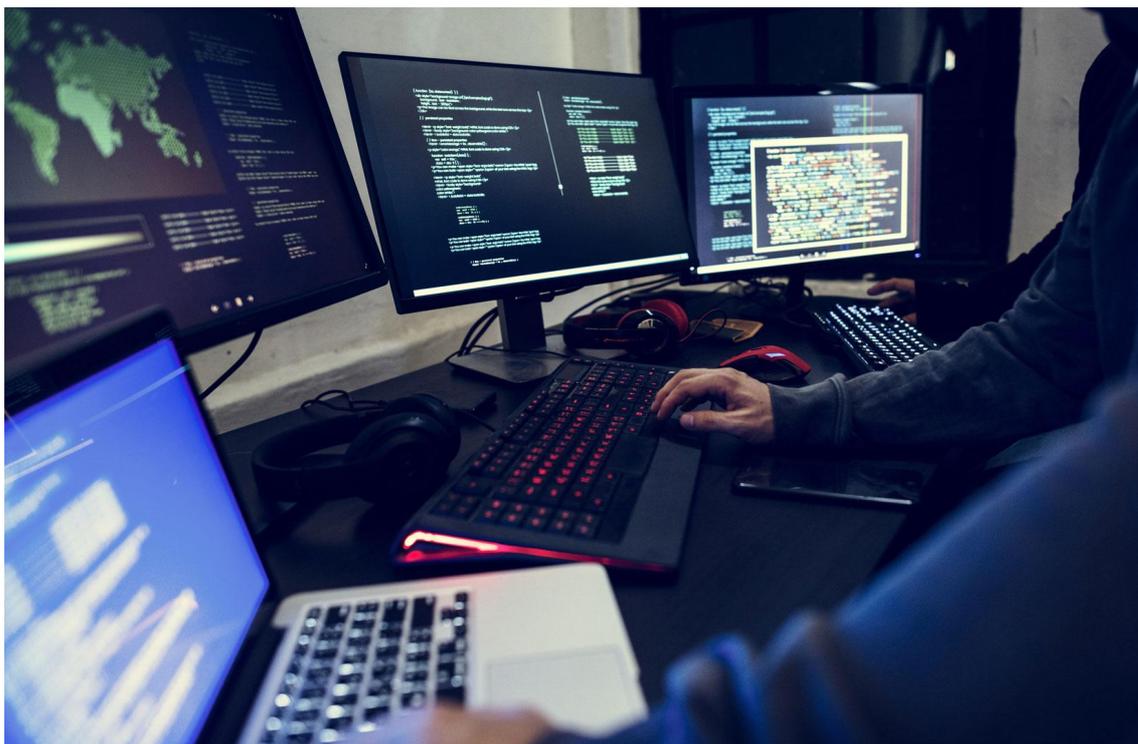
 (+33) 3 881 64504 (STR)

 (+32) 498 98 33 30

 [@EP_ForeignAff](https://twitter.com/EP_ForeignAff)

 [@EP_Defence](https://twitter.com/EP_Defence)

 gediminas.vilkas@europarl.europa.eu



Cyber-attacks are on the rise – and the EU must react © AP Images/European Union-EP