State of EU cyber defence capabilities

2020/2256(INI) - 07/10/2021 - Text adopted by Parliament, single reading

The European Parliament adopted by 591 votes to 65, with 26 abstentions, a resolution on the state of EU cyber defence capabilities.

State of EU cyber defence capabilities

Members stressed that a common cyber defence policy and increased cooperation at EU level aimed at developing common and improved cyber defence capabilities are essential elements in building a stronger European Defence Union. The borderless nature of cyber space, as well as the substantial number and increasing complexity of cyberattacks, require a **coordinated Union-level response**, including common Member State support capabilities and Member State support for measures in the EU's cyber diplomacy toolbox.

Parliament called on the EEAS and the Commission, in cooperation with the Member States, to further develop a **comprehensive set of measures** and a coherent policy on cyber security to enhance resilience, but also coordination on cyber defence.

It called for enhanced cooperation with the EU's civilian Computer Emergency Response Team (CERT-EU) to protect networks used by all EU institutions, bodies and agencies.

Noting the 2018 Cyber Defence Policy Framework's (CDPF) objective to setup an EU Military CERT-Network, Members called on the Member States to significantly increase classified information sharing capacities in order to facilitate information sharing where needed and useful, and to develop a European rapid and secure network to detect, asses and counter cyberattacks. They underlined the need to invest in cyber defence and cyber capabilities to strengthen the resilience and strategic capabilities of the Union and its Member States.

Strategic vision - Achieving cyber defence resilience

Parliament stressed that it was essential to **overcome the current fragmentation** and complexity of the overall cyber architecture within the EU and to define a common vision on how to ensure security and stability in cyberspace. It called for the creation of a **joint cyber security unit** to enhance cooperation and address the lack of information sharing between EU institutions, bodies and agencies.

Given that cyber defence capabilities often have a dual (civilian and military) dimension, Members recalled that technological innovation was mainly driven by private companies and that, therefore, **cooperation with the private sector** and civilian stakeholders should be strengthened.

Parliament also noted that, unlike other military fields, the infrastructure used to 'create' cyberspace is mainly in the hands of commercial entities established mostly outside the EU, which leads to industrial and technological dependence on third parties. The EU should therefore strengthen its technological sovereignty and stimulate innovation by investing in the ethical use of new security and defence technologies, such as artificial intelligence and quantum computing.

To overcome paralysis in the face of hybrid threats, Members considered that the EU should seek a legal solution that would provide for a right to collective defence and allow for the adoption of collective countermeasures by EU Member States on a voluntary basis.

Strengthening partnerships and the EU's role in the international context

In view of the systematically aggressive behaviour of China, Russia and North Korea in cyberspace and the numerous cyber-attacks against public institutions and private companies, Members believe that the EU and NATO should coordinate in areas where hostile actors threaten Euro-Atlantic security interests.

In particular, Members recommended:

- **closer cooperation between the EU and NATO**, especially on cyber defence interoperability requirements;

- better coordination on cyber defence between Member States, EU institutions, NATO Allies, the United Nations and the Organisation for Security and Cooperation in Europe (OSCE). In this context, they encouraged the further promotion of OSCE confidence-building measures in cyberspace;

- the development of a strong cyber partnership with the United Kingdom, which is at the forefront of the cyber defence arsenal. The Commission is invited to explore the possibility of re-launching a process aimed at establishing a formal and structured framework for future co-operation in this field.

All Member States and the EU are invited to play a leading role in discussions and initiatives under the auspices of the United Nations, including by proposing an action plan, and promoting responsible state behaviour in cyberspace.