State of EU cyber defence capabilities

2020/2256(INI) - 16/07/2021 - Committee report tabled for plenary, single reading

The Committee on Foreign Affairs adopted an own-initiative report by Urmas PAET (Renew, EE) on the state of EU cyber defence capabilities.

The report 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.

According to Members, 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 EUs cyber diplomacy toolbox, as well as intensified EU-NATO cooperation based on information sharing between cyber crisis response teams, the exchange of best practices, enhanced training, research and exercises.

The report 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 in order to enhance resilience, but also coordination on cyber defence. It called on 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.

Strategic Vision - Achieving Cyber Defence Resilience

The report stressed that it is essential to overcome the current fragmentation and complexity of the overall cyber architecture within the EU and to develop a common vision of how to achieve security and stability in cyberspace.

Members recommended, inter alia:

- increasing financial and cyber defence personnel resources, in particular cyber intelligence analysts and experts in cyber forensics, and their training in the areas of decision and policy making, policy implementation, cyber incident response and investigations, including the development of cyber skills;

- increase funding for CERT-EU (Computer Emergency Response Team) and the EU Intelligence and Situation Centre (INTCEN) and support for Member States in establishing and strengthening security operation centres (SOCs) in order to build a network of SOCs across the EU;

- promote partnerships with academia aimed at fostering cybersecurity R&D programmes in order to develop new common technologies, tools and skills applicable in both the civilian and the defence sectors;

- raise public awareness and improve citizens' skills to defend themselves against cyber-attacks.

The report called for the creation of a joint cyber unit to strengthen cooperation and address the lack of information sharing between EU institutions, bodies and agencies. It called for a European Digital Sovereignty programme to strengthen existing capabilities in cyber tools and encryption, based on European fundamental rights, with the aim of improving Europe's competitiveness in the cyber security market and boosting internal demand.

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.

According to the report, EU-NATO cooperation should focus on issues in the areas of cyber, hybrid threats, emerging and disruptive technologies, space, arms control and non-proliferation. Members called for EU-NATO cooperation to ensure resilient, affordable and secure broadband networks that meet European and national security standards and enable secure national and international information networks capable of encrypting sensitive data and communications.

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.