

Cyber defence

2018/2004(INI) - 25/05/2018 - Committee report tabled for plenary, single reading

The Committee on Foreign Affairs adopted the own-initiative report by Urmas PAET (ALDE, EE) on cyber defence.

The EU and the Member States face an unprecedented threat in the form of politically motivated, state-sponsored cyber-attacks as well as cyber-crime and terrorism. Given its current vulnerability mainly due to the fragmentation of European defence strategies, there is an urgent need to strengthen the EU's capabilities in the field of cyber defence.

Capability development for cyber defence: the report underlined that a common cyber defence policy should constitute core elements in the development of the European Defence Union (EDU). It called for a coherent development of cyber capacities across all EU institutions and bodies, as well as in the Member States, and for providing needed political and practical solutions to overcoming the remaining political, legislative and organisational obstacles to cooperation on cyber defence.

Members urged the Member States to cooperate closely in the development of their respective cyber defence, using a clear roadmap, thereby feeding into a process coordinated by the Commission, the European External Action Service (EEAS) and the European Defence Agency (EDA) with a view to better streamlining cyber defence structures across the Member States. A European secure network for critical information and infrastructure should be developed.

Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF): these are new initiatives with the necessary scope to foster an ecosystem that can provide opportunities for SMEs and start-up companies, and to facilitate cooperative projects in the cyber defence domain, and both will contribute to shape the regulatory and institutional framework. Member States are urged to make the best possible use of the framework provided by PESCO and the EDF to propose cooperation projects. They welcomed two cyber projects to be launched, 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.

Education and training: the report noted that a streamlined EU cyber defence education and training landscape would significantly mitigate threats. Members strongly support the Military Erasmus Programme and other common training and exchange initiatives aimed at enhancing the interoperability of the armed forces of the Member States and the development of a common strategic culture through an increased exchange of young military personnel. Further awareness raising and expertise in the area of cyber security is needed.

EU-NATO cooperation on cyber defence: the Council is called on to consider ways of providing, at soon as possible, Union-level support for integrating the cyber domain into Member States military doctrines, in a harmonised manner and in close cooperation with NATO. Members are convinced that increased cooperation between EU and NATO is important and useful in the area of cyber defence as a means to prevent, detect and deter cyber-attacks.

International norms: Members called for mainstreaming cyber defence capabilities into the CFSP and the external action of the EU and its Member States and called for closer coordination on cyber defence between the Member States, the EU institutions, NATO, the United Nations, the United States and other strategic partners, in particular as regards rules, norms and enforcement measures in cyber space. Member States should further implement the common and comprehensive EU approach to cyber diplomacy and existing cyber norms, and to draw up, together with NATO, EU-level criteria for, and definitions of what constitutes, a cyber-attack so as to improve the EU's ability to quickly come to a common position following an internationally wrongful act in the form of a cyber-attack.

Civil-military cooperation: noting the pivotal role that private cyber-security firms play in early warning and attribution of cyber-attacks, Members called on all stakeholders to reinforce knowledge transfer partnerships, implement appropriate business models and develop trust between companies and defence and civilian end-users. More practical support should be given to the European cyber security industry and other relevant economic actors, to reduce bureaucratic burdens, in particular for SMEs and to promote closer cooperation with university research organisations with a view to reducing dependencies on cyber security products from external sources and to creating a strategic supply chain inside the EU to enhance its strategic autonomy.

In this regard, Members encouraged the Commission to integrate cyber defence elements into a network of European cybersecurity competence and research centres, also in view of providing sufficient resources to dual use cyber capabilities and technologies within the next MFF.

The report also called for:

- a roadmap for a coordinated approach to European cyber defence;
- international cooperation and multilateral initiatives to build stringent cyber defence and cyber security frameworks to counter state capture by corruption, financial fraud, money laundering, the financing of terrorism;
- tackle the challenges posed by cyber terrorism and by cryptocurrencies and other alternative payment methods.

Institutional reinforcement: Members called for:

- the Member States to engage in more ambitious cooperation in the cyber domain within PESCO;
- the Member States and the VP/HR to present an EU white book on security and defence;
- the creation of an EU Council on Defence;
- the European Defence Fund to be maintained or even boosted in the next MFF, with a sufficient budget earmarked for cyber defence;
- increased resources to modernise and streamline cyber security and intelligence dissemination between the EEAS/European Union Intelligence and Situation Centre (INTCEN), the Council and the Commission.