Cyber defence

2018/2004(INI) - 13/06/2018 - Text adopted by Parliament, single reading

The European Parliament adopted by 476 votes to 151 with 36 abstentions, a resolution 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 EUs capabilities in the field of cyber defence.

Capability development for cyber defence: Parliament 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.

Members urged the Member States to cooperate closely in the development of their respective cyber defence, using a clear roadmap, 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.

Member States were urged to make the best possible use of the framework provided by the Permanent Structured Cooperation (PESCO) and the European Defence Fund to propose cooperation projects.

Members welcomed the two cyber projects to be launched in the framework of PESCO, namely the Cyber Threats and Incident Response Information Sharing Platform and the Cyber Rapid Response Teams and Mutual Assistance in Cyber Security. They hoped it would lead to the creation of a European cyber rapid response team, which would coordinate, detect and counter collective cyber threats.

Education and training: Parliament called on the EU and the Member States to strengthen their cooperation in education, training and exercises. It strongly support the Military Erasmus Programme and other common training and exchange initiatives among young military personnel. It stressed the need to strengthen awareness and expertise in the field of cybersecurity. All Member States should inform, educate and advise businesses, schools and citizens about cybersecurity and the major digital threats.

EU-NATO cooperation on cyber defence: the Council was 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 were convinced of the importance of increased cooperation between the EU and NATO as a means of preventing, detecting and deterring 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: Parliament called on all stakeholders to reinforce knowledge transfer partnerships, implement appropriate business models in order to create synergies and port solutions between the civilian and military markets in essence a European single market for cyber security and cyber-security products, with the view to preserving and strengthening the EUs strategic autonomy.

Member States should further support the European cyber security industry and reduce the administrative burden, 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.

The resolution 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 crypto currencies and other alternative payment methods.

At the institutional level, Parliament suggested that the Member States launch a new PESCO cyber cooperative programme with a view to supporting quick and effective planning, command and control of present and future EU operations and missions. This should lead to better coordination of operational capacities in cyber space, and may lead to the development of a common cyber defence command when the European Council so decides.