Fight against cybercrime

2017/2068(INI) - 26/07/2017 - Committee report tabled for plenary, single reading

The Committee on Civil Liberties, Justice and Home Affairs adopted the own-initiative report drawn up by Elissavet VOZEMBERG-VRIONIDI (EPP, EL) on the fight against cybercrime.

Background: Europol's assessment of the threat posed by organised crime on the Internet (IOCTA) of 28 September 2016 indicated that cybercrime (zombie networks and malware etc.) is increasing in intensity, complexity and causing ever-greater economic and social damage, affecting the fundamental rights of individuals. 80% of companies in Europe have experienced at least one cybersecurity incident.

Children who use the internet at an increasingly early age are particularly vulnerable to the risk of being groomed by paedophiles and other forms of online sexual exploitation.

Faced with these challenges, the report suggested clarifying the definitions of cybercrime to ensure that EU institutions and Member States share a common legal definitions.

On a general level, Members recommended the:

- rapid transposition of Directive 2011/93/EC on combating the sexual abuse and sexual exploitation of children and child pornography and the adoption of an action plan for the protection of children's rights online and offline in cyberspace;
- establishment of juridical measures to fight against the phenomenon of online violence against women and cyberbullying;
- guarantee that illegal online content should be removed immediately by due legal process.

To be effective, cybersecurity strategies should be based on fundamental freedoms and rights.

Prevention: in the context of the review of the EU's cybersecurity strategy, the Commission is invited to:

- identify network and information security vulnerabilities of European Critical Infrastructure, promote the development of resilient systems and assess the situation with regard to the fight against cybercrime in the Union and the Member States;
- launch awareness-raising, information and prevention campaigns (with educational programmes) to ensure that all citizens, in particular children and other vulnerable users, but also central and local governments, and private sector actors, especially SMEs, are aware of the risks posed by cybercrime.

Member States should intensify the exchange of information, through Eurojust, Europol and ENISA, as well as best practice sharing via the European CSIRT (Cyber Security Incident Response Teams) and the CERTs (Computer Emergency Response Teams), with regard to the problems they face in the fight against cybercrime.

Enhance the responsibility of service providers: Members called for closer cooperation between competent authorities and service providers to accelerate mutual legal assistance and mutual recognition procedures in the areas of competence provided for in the European legal framework. Providers of electronic communications services established in a third country should designate in writing representatives in the Union.

In view of innovation trends and the growing accessibility of Internet of Things (IoT) devices, Members stated that attention must be paid to the safety of all devices and to promote the security by design approach.

They stressed the need to protect law enforcement databases from security incidents and unlawful access. They also encouraged service providers to adhere to the Code of Conduct on Countering Illegal Hate Speech Online.

Strengthening police and judicial cooperation: the report stressed the need to allow law enforcement authorities to have lawful access to relevant information, in the limited circumstances where such access is necessary and proportionate for reasons of security and justice.

Members called on the not to impose any obligation on encryption providers that would result in the weakening or compromising of the security of their networks or services, such as the creation or facilitation of back doors.

Feasible solutions must be offered where finding them is imperative for justice and security.

According to Members, lawful interception can be a highly effective measure to combat unlawful hacking, on condition that it is necessary, proportionate, based on due legal process and in full compliance with fundamental rights and EU data protection law and case law.

Electronic evidence: the report called for a common European approach to criminal justice. It stressed the need to find means to secure and obtain e-evidence more rapidly, as well as the importance of close cooperation between law enforcement authorities, third countries and service providers active on European territory.

In order to strengthen capacity-building at European level, the report called on ENISA to continuously evaluate the threat level and encouraged the Commission to invest in the IT capacity as well as the defence and resilience of the critical infrastructure of the EU institutions in order to reduce the EUs vulnerability to serious cyberattacks originating from large criminal organisations.