# Procedure file

## Basic information

| | | |
|---|---|---|
| INI - Own-initiative procedure | 2017/2068(INI) | Procedure completed |
| Fight against cybercrime<br><br>Subject<br>3.30.07 Cybersecurity, cyberspace policy<br>3.30.25 International information networks and society, internet<br>7.30.30 Action to combat crime | | |

## Key players

| | | | |
|---|---|---|---|
| European Parliament | Committee responsible | Rapporteur | Appointed |
| | LIBE Civil Liberties, Justice and Home Affairs | | 30/01/2017 |
| | | VOZEMBERG-VRIONIDI Elissavet | |
| | | Shadow rapporteur | |
| | | S&D DALLI Miriam | |
| | | ECR PROCTER John | |
| | | GRIESBECK Nathalie | |
| | | ALBRECHT Jan Philipp | |
| | Committee for opinion | Rapporteur for opinion | Appointed |
| | INTA International Trade | The committee decided not to give an opinion. | |
| | ITRE Industry, Research and Energy | The committee decided not to give an opinion. | |
| | IMCO Internal Market and Consumer Protection | | 09/02/2017 |
| | | ECR VAN BOSSUYT Anneleen | |
| Council of the European Union | Council configuration | Meeting | Date |
| | Justice and Home Affairs (JHA) | 3539 | 18/05/2017 |
| European Commission | Commission DG | Commissioner | |
| | Migration and Home Affairs | AVRAMOPOULOS Dimitris | |

## Key events

| | | | |
|---|---|---|---|
| 18/05/2017 | Resolution/conclusions adopted by Council | | |
| 18/05/2017 | Committee referral announced in Parliament | | |
| 11/07/2017 | Vote in committee | | |

| | | | |
|---|---|---|---|
| 26/07/2017 | Committee report tabled for plenary | A8-0272/2017 | Summary |
| 02/10/2017 | Debate in Parliament | | |
| 03/10/2017 | Results of vote in Parliament | | |
| 03/10/2017 | Decision by Parliament | T8-0366/2017 | Summary |
| 03/10/2017 | End of procedure in Parliament | | |

## Technical information

| | |
|---|---|
| Procedure reference | 2017/2068(INI) |
| Procedure type | INI - Own-initiative procedure |
| Procedure subtype | Initiative |
| Legal basis | Rules of Procedure EP 54 |
| Other legal basis | Rules of Procedure EP 159 |
| Stage reached in procedure | Procedure completed |
| Committee dossier | LIBE/8/09854 |

## Documentation gateway

| | | | | | |
|---|---|---|---|---|---|
| Committee draft report | | PE604.566 | 11/05/2017 | EP | |
| Amendments tabled in committee | | PE606.071 | 09/06/2017 | EP | |
| Amendments tabled in committee | | PE606.072 | 09/06/2017 | EP | |
| Committee opinion | IMCO | PE606.009 | 13/06/2017 | EP | |
| Committee report tabled for plenary, single reading | | A8-0272/2017 | 26/07/2017 | EP | Summary |
| Text adopted by Parliament, single reading | | T8-0366/2017 | 03/10/2017 | EP | Summary |
| Commission response to text adopted in plenary | | SP(2017)778 | 22/01/2018 | EC | |

# Fight against cybercrime

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.

## Fight against cybercrime

The European Parliament adopted by 603 votes to 27, with 39 abstentions, a resolution 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 scale. 80% of companies in Europe have experienced at least one cybersecurity incident.

Children are particularly vulnerable to the risk of being groomed by paedophiles and other forms of online sexual exploitation. A considerable number of cybercrimes remain unprosecuted and unpunished.

Given the cross-border nature of cybercrime as well as the common cybersecurity threats faced by the EU, Parliament called for enhanced cooperation and information exchange between police and judicial authorities and cybercrime experts is essential for conducting effective investigations in cyberspace and obtaining electronic evidence.

On a general level, Members suggested streamlining common definitions of cybercrime, while stressing that the fight against cybercrime should be first and foremost about safeguarding and hardening critical infrastructures, including, among others, energy and electricity supply and financial structures. They strongly condemned any system interference undertaken or directed by a foreign nation or its agents to disrupt the democratic process of another country.

Parliament also recommended:

- adopting an action plan for the protection of childrens rights online and offline in cyberspace;
- putting in place all the necessary legal measures to combat the phenomenon of online violence against women and cyberbullying;
- giving Eurojust and Europol the means to improve the identification of victims and fight criminal networks of sexual offenders and accelerate the detection, analysis and reporting of child pornography material both online and offline;
- ensure that illegal online content is removed immediately by legal means.

Prevention: in the context of EU's cybersecurity strategy review, 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;
- promote security measures such as encryption and anonymisation tools.

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). They should also

invest in education as a solution to the lack of qualified IT professionals working on cybersecurity.

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

In view of 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.

Member States are urged to set up CERTs to which businesses and consumers can report malicious emails and websites as foreseen by the network and information security Directive (NIS).

Strengthening police and judicial cooperation: Parliament 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.

Member States should 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: Parliament 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.

The Commission should propose a European legal framework for e-evidence including harmonised rules to determine the status of service providers, whether domestic or foreign, and oblige them to respond to requests from other Member States. This framework should provide for adequate safeguards concerning the rights and freedoms of all parties concerned.

Lastly, Parliament deplored the absence of binding international legislation on cybercrime and urged the Member States and the European institutions to work towards establishing a convention on the matter.