European Parliament
2014-2019

Committee on Civil Liberties, Justice and Home Affairs

2017/2068(INI)

7.5.2017

DRAFT REPORT

on the fight against cybercrime
(2017/2068(INI))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Elissavet Vozemberg-Vrionidi

CONTENTS

Page

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

on the fight against cybercrime
(2017/2068(INI))

The European Parliament,

– having regard to Articles 2, 3 and 6 of the Treaty on European Union (TEU),

– having regard to Articles 16, 67, 70, 72, 73, 75, 82, 83, 84, 85, 87 and 88 of the Treaty on the Functioning of the European Union (TFEU),

– having regard to Articles 1, 7, 8, 11, 21, 24 and 52 of the Charter of Fundamental Rights of the European Union (CFR),

– having regard to Council Framework Decision of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment[1],

– having regard to the Budapest Convention on Cybercrime of 23 November 2001[2],

– having regard to Regulation (EC) No 460/2004 of 10 March 2004 of the European Parliament and of the Council establishing the European Network and Information Security Agency[3],

– having regard to Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection[4],

– having regard to Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector[5],

– having regard to Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA[6],

– having regard to the Joint Communication of 7 February 2013 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions by the European Commission and the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy, entitled ‘Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace’ (JOIN(2013)0001),

– having regard to Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council

[1] OJ L 149, 2.6.2001, p. 1.
[2] Council of Europe, European treaty Series, No 185, 23.11.2001.
[3] OJ L 77, 13.3.2004, p. 1.
[4] OJ L 345, 23.12.2008, p. 75.
[5] OJ L 201, 31.7.2002, p. 37.
[6] OJ L 335, 17.12.2011, p. 1.

Framework Decision 2005/222/JHA[1],

– having regard to Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 on the European Investigation Order in criminal matters (the EIO Directive)[2],

– having regard to its resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace[3],

– having regard to the Commission communication of 28 April 2015 entitled 'A Digital Single Market Strategy for Europe' (COM(2015)0192),

– having regard to the Commission communication of 28 April 2015 entitled 'The European Agenda on Security' (COM(2015)0185) and the subsequent follow-up progress reports entitled 'Towards an effective and genuine Security Union',

– having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR)[4],

– having regard to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA[5],

– having regard to Regulation (EU) 2016/794 of the European Parliament and the Council of 11 May 2016 on the European Agency for Law Enforcement Cooperation (Europol)[6],

– having regard to the Commission decision of 5 July 2016 on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation (C(2016)4400),

– having regard to the Joint Communication of 6 April 2016 to the European Parliament and the Council entitled 'Joint framework on countering hybrid threats: a European Union response' (JOIN(2016)0018),

– having regard to Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of

[1] OJ L 218, 14.8.2013, p.8.
[2] OJ L 130, 1.5.2014, p. 1.
[3] OJ C 93, 9.3.2016, p. 112.
[4] OJ L 119, 4.5.2016, p. 1.
[5] OJ L 119, 4.5.2016, p. 89.
[6] OJ L 135, 24.5.2016, p. 53

network and information systems across the Union[1],

– having regard to the final report of the T-CY Cloud Evidence Group of the Council of Europe entitled ‘Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY’ of 16 September 2016,

– having regard to the Europol Serious and Organised Crime Threat Assessment (EU SOCTA) of 28 February 2017 and the Internet Organised Crime Threat Assessment (IOCTA) of 28 September 2016,

– having regard to the judgment of the Court of Justice of the European Union (CJEU) in case C-203/15 (TELE2 judgment) of 21 December 2016[2],

– having regard to Directive 2017/541/EU of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA[3],

– having regard to rule 52 of its Rules of Procedure,

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs (A8-0000/2017),

A. whereas cybercrime is causing increasingly significant social and economic damage affecting the fundamental rights of individuals, posing threats to the rule of law in cyberspace and endangering the stability of democratic societies;

B. whereas the lines between cybercrime, cyber espionage, cyber warfare, cyber sabotage and cyber terrorism are becoming increasingly blurred; whereas cybercrimes can target individuals, public or private entities and cover a wide range of offences, including privacy breaches, copyright infringement, child pornography, online incitement to hate, the dissemination of fake news with malicious intent, financial crime and fraud, as well as illegal system interference;

C. whereas the 2016 IOCTA reveals that cybercrime is increasing in intensity, complexity and magnitude, that reported cybercrime exceeds traditional crime in some EU countries, that it extends to other areas of crime, such as human trafficking, that there has been a growing misuse of encryption and anonymisation tools and that ransomware attacks outnumber traditional malware threats such as Trojans;

D. the key focus of cyber-attacks remains on sensitive personal information such as health or financial records, but attacks on industrial control systems and networks aimed at destroying economic structures and destabilising societies are growing in number; whereas the majority of international requests for data are related to fraud and financial crime, followed by violent and serious crime;

E. whereas a considerable number of cybercrimes remain unprosecuted and unpunished,

[1] OJ L 194, 19.7.2016, p. 1.
[2] Judgment of the Court of Justice of 21 December 2016, *Tele2 Sverige AB* v *Post- och telestyrelsen* and *Secretary of State for the Home Department* v *Tom Watson and Others*, C-203/15, ECLI:EU:C:2016:970.
[3] OJ L 88, 31.3.2017, p. 6.

due in part to significant underreporting, long detection periods allowing cybercriminals to develop multiple entries/exits or backdoors, difficult access to e-evidence, problems in obtaining it and with its admissibility in court, as well as complex procedures and jurisdictional challenges related to the cross-border nature of cybercrimes;

F. whereas the TELE2 judgment of the CJEU imposes stringent limits on police and judicial access to the data of cybercrime suspects;

G. whereas children are particularly vulnerable to online grooming and other forms of sexual exploitation online and therefore require special protection;

H. whereas awareness about the risks posed by cybercrime has increased, but precautionary measures, both on the part of individual users and of business, remain absent;

I. whereas the constantly growing interconnectedness of people, places and things makes Internet of Things (IoT) devices an ideal target for cybercriminals;

General considerations

1. Stresses that the sharp increase in ransomware, botnets and the unauthorised impairment of computer systems has an impact on the availability and integrity of personal data, as well as on the protection of privacy and fundamental freedoms;

2. Reiterates the importance of the legal measures taken at European level to harmonise the definition of offences linked to attacks against information systems as well as to child sexual exploitation online and to oblige the Member States to set up a system for the recording, production and provision of statistical data on these offences;

3. Deplores that cyber-attacks against businesses often remain undetected or unreported; believes that the obligation to disclose security breaches introduced by the GDPR will help to address this problem;

4. Stresses that the constantly changing nature of the cyber-threat landscape presents all stakeholders with serious legal and technological challenges; points, in particular, to the increasing misuse of privacy-enhancing technologies such as onion-routing and the Darknet, as well as to the growing threats posed by hackers sponsored by non-friendly foreign states or extremist political or religious organisations;

5. Notes that the recourse of extremists to cybercrime tools and services is still limited; highlights, however, that this is likely to change in light of the growing links between terrorism and organised crime and the wide availability of firearms and explosive precursors on the Darknet;

6. Acknowledges that technological advances in encryption allow legitimate users to better protect their data, but points out that malicious users deploy the same techniques to conceal their criminal activities and identities;

7. Calls on the Member States to step up their efforts in relation to victim identification and victim-centred services;

Prevention

8. Calls on the Commission, in the context of the review of the European cybersecurity strategy, to assess the situation regarding the fight against cybercrime in the European Union and the Member States, in order to achieve a better understanding of the trends and developments in relation to offences in cyberspace;

9. Stresses that cyber-resilience is key in preventing cybercrime and should therefore be given the highest priority; calls for a comprehensive European approach on the fight against cybercrime that is compatible with fundamental rights, data protection, cybersecurity, consumer protection and e-commerce;

10. Welcomes, in this regard, the investment of EU funds in research projects such as the public-private partnership (PPP) on cybersecurity, to foster European cyber-resilience through innovation and capacity building;

11. Urges the Member States to step up information exchanges on the challenges they face in the fight against cybercrime, as well as on solutions to address them;

12. Is concerned by the Europol finding that the majority of successful attacks are attributable to a lack of user-awareness, as well as insufficient security;

13. Calls on the Commission and the Member States to launch awareness-raising campaigns to ensure that citizens, in particular children and other vulnerable users, and the private sector are aware of the risks posed by cybercrime, and to promote the use of security measures such as encryption;

14. Stresses that businesses should conduct regular vulnerability assessments, fix existing vulnerabilities in their products or services and consistently report cyber-attacks;

15. Urges the Member States to invest in making their critical infrastructure and associated data more secure in order to withstand cyber-attacks;

Enhancing responsibility and liability of the service providers

16. Considers enhanced cooperation with service providers to be a key factor in accelerating and streamlining mutual legal assistance and mutual recognition procedures;

17. Believes that innovation should not be hampered by unnecessary red tape for software developers and hardware producers; encourages the private sector to implement voluntary measures aimed at bolstering trust in the security of software and devices, such as the IoT trust label;

18. Calls on the Commission to put forward legislative measures setting out clear definitions and minimum penalties for the dissemination of fake news and online incitement to hate, the related obligations of internet service providers and penalties in the event of non-compliance;

19. Calls on the Commission to investigate the legal scope for improving the accountability of service providers and for imposing an obligation to respond to foreign EU law-

enforcement requests;

20. Calls on the Member States to impose the same encryption obligations on online service providers as those, which apply to providers of traditional telecommunications services;

21. Underlines that illegal online content should be removed immediately; welcomes, in this context, the progress achieved concerning the blocking and removal of illegal content online, but stresses the need for a stronger commitment on the part of platform service providers to respond quickly and effectively;

Strengthening police and judicial cooperation

22. Is concerned that a considerable number of cybercrimes remain unpunished; emphasises the need to allow lawful access to relevant information, even if it has been encrypted, if such access is imperative for reasons of security and justice;

23. Urges the Member States to exchange best practices regarding the circumvention of encryption and to cooperate, in consultation with the judiciary, in aligning the conditions for the lawful use of investigative tools online;

24. Stresses that lawful hacking must be a measure of last resort, which has to be necessary, proportionate, and in full compliance with fundamental rights and EU data protection and case law; calls on all Member States to establish clear rules regarding the authorisation process for lawful hacking activities, including restrictions on the use and duration of lawful hacking tools, to set up an oversight mechanism, and to provide effective legal remedies for the targets of these hacking activities;

25. Calls on the Member States to notify each other about breaches of their territorial sovereignty as part of investigations conducted due to lack of information about the location of the hacked device;

26. Stresses the need to minimise the risks posed to the privacy of internet users by leaks of exploits or tools used by law-enforcement authorities as part of their legitimate investigations;

27. Emphasises that judicial and law enforcement authorities have to be equipped with sufficient capabilities and funding to respond effectively to cybercrime;

28. Underlines that the patchwork of separate, territorially defined national jurisdictions causes difficulties in determining the applicable law in transnational interactions and gives rise to legal uncertainty, thereby preventing cooperation across borders, which is necessary to deal efficiently with misuses online;

e-Evidence

29. Underlines that a common European approach to criminal justice in cyberspace is a matter of priority, as it will improve the enforcement of the rule of law in cyberspace and facilitate the obtaining of e-evidence in criminal proceedings;

30. Underlines the importance of close cooperation between law enforcement authorities and the private sector on the issue of access to e-evidence; urges the Member States

concerned to eliminate criminal law provisions prohibiting domestic service providers from responding to foreign law enforcement requests;

31. Calls on the Commission to put forward a European legal framework for e-evidence, including harmonised rules to determine the status of a provider as domestic or foreign, and to impose an obligation on service providers to respond to requests from third countries, with a view to ensuring legal certainty for stakeholders and removing obstacles to cooperation;

32. Calls on the Member States to implement fully the EIO Directive for the purposes of the effective securing and obtaining of e-evidence in the EU, as well as to include specific provisions relating to cyberspace in their national penal codes in order to facilitate the admissibility of e-evidence in court and to issue clearer guidance to judges regarding the penalisation of cybercrime;

Capacity-building at European level

33. Recognises the important contribution of the Justice and Home Affairs (JHA) agencies, especially the European Cybercrime Centre (EC3) of Europol and Eurojust, as well as the European Union Agency for Network and Information Security (ENISA), to the fight against cybercrime;

34. Calls on Europol to support national law enforcement authorities in setting up secure and adequate transmission channels;

35. Calls on the European Union Agency for Law Enforcement Training (CEPOL) and the European Judicial Training Network to extend their offer of training courses dedicated to cybercrime-related topics to competent law enforcement bodies and judicial authorities across the Union;

36. Calls for sufficient funding and posts to be made available to the European Union's Judicial Cooperation Unit (Eurojust) to allow the agency to cope with its increasing workload, as well as to develop and strengthen further its support to national cybercrime prosecutors in cross-border cases, including via the recently established European Judicial Cybercrime Network;

Improved cooperation with third countries

37. Highlights the importance of close cooperation with third countries in the global fight against cybercrime, including through the exchange of best practices, joint investigations, capacity-building, and mutual legal assistance;

38. Underlines that strategic and operational cooperation agreements between Europol and third countries facilitate both the exchange of information and practical cooperation; invites Europol to conclude agreements with all countries listed in the annex to the Europol regulation in due course;

39. Takes note of the fact that the highest number of law enforcement requests is sent to the United States and Canada; is concerned that the voluntary disclosure rate of big US service providers in response to requests from European criminal justice authorities falls

short of 60 %;

40. Calls on the Commission to put forward concrete measures to address impediments to the exchange of information between European law enforcement authorities and third countries, notably the quick obtaining, upon a court decision, of relevant evidence, subscriber-related information as well as detailed meta- and content data (if not encrypted) from law-enforcement authorities and/or service providers with a view to improving mutual legal assistance;

41. Supports the capacity-building assistance provided by the EU to Eastern Neighbourhood countries, given that many cyber-attacks originate in them;

°

° °

42. Instructs its President to forward this resolution to the Council and the Commission.