European Parliament
2014-2019

Plenary sitting

A8-0272/2017

25.7.2017

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, 16, 17, 21, 24, 41, 47, 48, 49, 50 and 52 of the Charter of Fundamental Rights of the European Union (CFR),

– having regard to the UN Convention on the Rights of the Child of 20 November 1989,

– having regard to the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, of 25 May 2000,

– having regard to the Stockholm Declaration and Agenda for Action, adopted at the 1st World Congress against the Commercial Sexual Exploitation of Children, to the Yokohama Global Commitment adopted at the 2nd World Congress against the Commercial Sexual Exploitation of Children, and to the Budapest Commitment and Plan of Action, adopted at the preparatory conference to the 2nd World Congress against the Commercial Sexual Exploitation of Children,

– having regard to the Council of Europe Convention of 25 October 2007 on the Protection of Children against Sexual Exploitation and Sexual Abuse,

– having regard to its resolution of 20 November 2012 on protecting children in the digital world[1],

– having regard to its resolution of 11 March 2015 on child sexual abuse online[2],

– having regard to the Council Framework Decision of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment[3],

– having regard to the Budapest Convention on Cybercrime of 23 November 2001[4] and the Additional Protocol thereto,

– 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[5],

– having regard to Council Directive 2008/114/EC of 8 December 2008 on the

[1] OJ C 419, 16.12.2015, p. 33.
[2] OJ C 316, 30.8.2016, p. 109.
[3] OJ L 149, 2.6.2001, p. 1.
[4] Council of Europe, European Treaty Series, No 185, 23.11.2001.
[5] OJ L 77, 13.3.2004, p. 1.

identification and designation of European critical infrastructures and the assessment of the need to improve their protection[1],

– 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[2],

– 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[3],

– 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 Framework Decision 2005/222/JHA[4],

– 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)[5],

– having regard to the ruling of the Court of Justice of the European Union of 8 April 2014 invalidating the Data Retention Directive,

– having regard to its resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace[6],

– 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 the Report of the conference on jurisdiction in cyberspace held in Amsterdam on 7 and 8 March 2016,

– 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

[1] OJ L 345, 23.12.2008, p. 75.
[2] OJ L 201, 31.7.2002, p. 37.
[3] OJ L 335, 17.12.2011, p. 1.
[4] OJ L 218, 14.8.2013, p.8.
[5] OJ L 130, 1.5.2014, p. 1.
[6] OJ C 93, 9.3.2016, p. 112.

processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[1],

– 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[2],

– 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)[3],

– 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 the Commission Communication entitled ‘European Strategy for a Better Internet for Children’ (COM(2012)0196), and to the Commission report of 6 June 2016 entitled 'Final evaluation of the multi-annual EU programme on protecting children using the Internet and other communication technologies (Safer Internet)' (COM(2016)0364),

– having regard to the Europol and ENISA Joint Statement of 20 May 2016 on lawful criminal investigation that respects 21st Century data protection,

– having regard to the Council conclusions of 9 June 2016 on the European Judicial Cybercrime Network,

– 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 network and information systems across the Union[4],

– having regard to the ENISA’s Opinion Paper of December 2016 on Encryption – Strong Encryption Safeguards our Digital Identity,

– 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,

[1] OJ L 119, 4.5.2016, p. 1.
[2] OJ L 119, 4.5.2016, p. 89.
[3] OJ L 135, 24.5.2016, p. 53
[4] OJ L 194, 19.7.2016, p. 1.

– having regard to the work of the Joint Cyber Crime Action Taskforce (J-CAT),

– 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[1],

– 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[2],

– 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 and the opinion of the Committee on the Internal Market and Consumer Protection (A8-0272/2017),

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 cybercrime is a growing problem in the Member States;

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 the use of encryption and anonymisation tools for criminal purposes is increasing and that ransomware attacks outnumber traditional malware threats such as trojans;

D. whereas there was an increase of 20 % in the attacks on the Commission's servers in 2016 compared to 2015;

E. whereas the vulnerability of computers to attack has its origins in the unique way information technology has developed over the years, the speed at which business has grown online, and lack of government action;

F. whereas there is an ever-growing black market in computerised extortion, the use of hired botnets and hacking, and stolen digital goods;

G. whereas the key focus of cyber-attacks continues to be malware, such as banking trojans, but attacks on industrial control systems and networks aimed at destroying critical infrastructure and economic structures as well as destabilising societies, as was the case of the 'WannaCry' ransomware attack of May 2017, are also growing in number and impact and thus pose an increasing threat to security, defence and other important sectors; whereas the majority of international law enforcement requests for

[1] 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.
[2] OJ L 88, 31.3.2017, p. 6.

data are related to fraud and financial crime, followed by violent and serious crime;

H. whereas, while the constantly growing interconnectedness of people, places and things brings many benefits, it increases the risk of cybercrime; whereas devices connected to the Internet of Things (IoT), which include smart grids, connected fridges, cars, medical tools or aids, are often not as well protected as traditional internet devices and are thus an ideal target for cybercriminals, especially because the regime for security updates for connected devises is often patchy or lacking completely; whereas hacked IoT devices that have or can control physical actuators may represent a concrete threat to the lives of human beings;

I. whereas an effective legal framework for data protection is critical for building confidence and trust in the online world, allowing consumers as well as businesses to fully reap the benefits of the digital single market and to address cybercrime;

J. whereas companies alone cannot deal with the challenge of making the connected world more secure, and government should contribute to cyber security through regulation and the provision of incentives encouraging safer behaviour by users;

K. 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, child sexual abuse online, public incitement to violence and hatred, sabotage, espionage, financial crime and fraud, such as payment fraud, theft and identity theft as well as illegal system interference;

L. whereas the World Economic Forum's Global Risks Report 2017 lists massive incident of data fraud and theft as one of the five major global risks in terms of likelihood;

M. whereas a considerable number of cybercrimes remain unprosecuted and unpunished; whereas there is still 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;

N. whereas the Council in its conclusions of June 2016 highlighted that, given the cross-border nature of cybercrime as well as the common cybersecurity threats faced by the EU, 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;

O. whereas the annulment of the Data Retention Directive by the CJEU in its ruling of 8 April 2014 as well as the prohibition of general, indiscriminate and non-targeted data retention as confirmed by the ruling of the CJEU in its TELE2 judgment of 21 December 2016 imposes stringent limitations on the processing of bulk telecommunications data as well as on the access of competent authorities to such data;

P. whereas the Maximillian Schrems judgment of the CJEU highlights that mass surveillance is a breach of fundamental rights;

Q. whereas the fight against cybercrime must respect the same procedural and substantive guarantees and fundamental rights, namely regarding data protection and freedom of speech, just as the fight against any other area of crime;

R. whereas children use the internet at an increasingly early age and are particularly vulnerable to falling victim to grooming and other forms of sexual exploitation online (cyber bullying, sexual abuse, sexual coercion and extortion), misappropriation of personal data as well as dangerous campaigns intended to promote various kinds of self-harm, as in the case of 'blue whale', and therefore require special protection; whereas online perpetrators can find and groom victims faster via chat rooms, emails, online games and social networking sites and hidden peer-to-peer (P2P) networks remain the central platforms for child sex offenders to access, communicate, store and share child sexual exploitation material and to track new victims without being detected;

S. whereas the growing trend of sexual coercion and extortion is still not being sufficiently studied or reported, mostly owing to the nature of the crime, which causes the victims to feel shame and guilt;

T. whereas live distant child abuse is being reported as a growing threat; whereas live distant child abuse has the most obvious links with the commercial distribution of child sexual exploitation materials;

U. whereas a recent study by the National Crime Agency in the UK found that younger persons who engage in hacking activities are less motivated by money and often attack computer networks to impress friends or to challenge a political system;

V. whereas awareness about the risks posed by cybercrime has increased, but precautionary measures taken by individual users, public institutions and businesses, remain wholly inadequate, primarily due to lack of knowledge and resources;

W. whereas the fight against cybercrime and against illegal activities online should not obscure the positive aspects of a free and open cyberspace, offering new possibilities for the sharing of knowledge and the promotion of political and social inclusion worldwide;

General considerations

1. Stresses that the sharp increase in ransomware, botnets and the unauthorised impairment of computer systems has an impact on the security of individuals, the availability and integrity of their personal data, as well as on the protection of privacy and fundamental freedoms and the integrity of critical infrastructure including, but not limited to, energy and electricity supply and financial structures such as the stock exchange; recalls, in this context, that the fight against cybercrime is a priority under the European Agenda on Security of 28 April 2015;

2. Stresses the need to streamline common definitions of cybercrime, cyber warfare, cybersecurity, cyber harassment and cyberattacks to ensure that the EU institutions and EU Member States share a common legal definition;

3. Underlines that the fight against cybercrime should be first and foremost about safeguarding and hardening critical infrastructures and other networked devices, and not

only about pursuing repressive measures;

4. 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 sexual abuse and exploitation of children online and to oblige the Member States to set up a system for the recording, production and provision of statistical data on these offences, in order to fight against these kinds of crime more effectively;

5. Strongly urges those Member States that have not yet done so to swiftly and properly transpose and implement Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography; calls on the Commission to strictly monitor and ensure its full and effective implementation, and to report back to Parliament and to the committee responsible on its findings in a timely manner, replacing at the same time Council Framework Decision 2004/68/JHA; stresses that Eurojust and Europol must be given appropriate resources to improve the identification of victims, to fight organised networks of sexual abusers and to accelerate the detection, analysis and referral of child abuse material both online and offline;

6. Deplores the fact that 80 % of companies in Europe have experienced at least one cyber security incident and that cyber-attacks against businesses often remain undetected or unreported; recalls that various studies estimate the annual cost of cyber-attacks to be significant to the world economy; believes that the obligation to disclose security breaches and to share information on risks, introduced by 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 (the General Data Protection Regulation (GDPR))[1] and 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 network and information systems across the Union (the Directive on security of network and information systems (NIS Directive))[2], will help to address this problem by providing support for businesses, especially SMEs;

7. Stresses that the constantly changing nature of the cyber-threat landscape presents all stakeholders with serious legal and technological challenges; believes that new technologies should not be seen as a threat and acknowledges that technological advances on encryption will improve the overall security of our information systems, including by allowing end-users to better protect their data and communications; points out, however, that there are still notable gaps in securing communications and that techniques such as onion routing and hidden networks can be used by malicious users, including terrorists and child sex offenders, hackers sponsored by non-friendly foreign states or extremist political or religious organisations for criminal purposes, in particular to conceal their criminal activities or identities, causing serious challenges for investigations;

8. Is highly concerned about the recent global ransomware attack, which appeared to affect tens of thousands of computers in nearly 100 countries and numerous organisations, including the National Health Service (NHS) in the UK, the highest-profile victim of

[1] OJ L 119, 4.5.2016, p. 1.
[2] OJ L 194, 19.7.2016, p. 1.

this extensive malware hit; recognises, in this context, the important work of the No More Ransom (NMR) initiative which provides over 40 free decryption tools allowing victims of ransomware worldwide to decrypt their affected devices;

9. Underlines that hidden networks and onion-routing also provide a free space for journalists, political campaigners and human rights defenders in certain countries to avoid detection by repressive state authorities;

10. Notes that the recourse of criminal and terrorist networks 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 hidden networks;

11. Strongly condemns any system interference undertaken or directed by a foreign nation or its agents to disrupt the democratic process of another country;

12. Underlines that cross-border requests for domain seizures, content takedowns and access to user data pose serious challenges that require urgent action, as the stakes involved are high; stresses, in this context, that international human rights frameworks, which apply online as well as offline, represent a substantive benchmark at global level;

13. Calls on the Member States to ensure that victims of cyber-attacks can fully benefit from all the rights enshrined in Directive 2012/29/EU, and to step up their efforts in relation to victim identification and victim-centred services, including through continued support for the Europol Task Force Victim ID; calls on the Member States in cooperation with Europol to set up related platforms as a matter of urgency with the aim of ensuring that all internet users know how to appeal for help when they are illegally targeted online; calls on the Commission to issue a study on to the implications of cross-border cybercrime on the basis of Directive 2012/29/EU;

14. Underlines that Europol's 2014 IOCTA refers to the need for more efficient and effective legal tools, taking into account the current limitations of the Mutual Legal Assistance Treaty (MLAT) process, and also advocates further harmonisation of legislation across the EU where appropriate;

15. Underlines that cybercrime severely undermines the functioning of the digital single market by reducing trust in digital service providers, undermining cross-border transactions and seriously harming the interests of consumers of digital services;

16. Stresses that cybersecurity strategies and measures can only be sound and effective if they are based on fundamental rights and freedoms, as enshrined in the Charter of Fundamental Rights of the European Union, and on the EU's core values;

17. Stresses that there is a legitimate and strong need to protect communications between individuals and between individuals and public and private organisations in order to prevent cybercrime; highlights that strong cryptography can help fulfil this need; stresses, furthermore, that limiting the use of or weakening the strength of cryptographic tools will create vulnerabilities that can be exploited for criminal purposes and lower trust in electronic services, which in turn will damage civil society and industry alike;

18. Calls for an action plan to protect children's rights online and offline in cyberspace, and recalls that in fighting cybercrime law enforcement authorities need to pay special attention to crimes against children; stresses, in this connection, the need to strengthen judicial and police cooperation among the Member States, and with Europol and its European Cybercrime Centre (EC3), with a view to preventing and combating cybercrime and in particular the online sexual exploitation of children;

19. Urges the Commission and the Member States to put in place all juridical measures to fight against the phenomenon of online violence against women and cyberbullying; calls, in particular, for the EU and the Member States to combine forces in order to create a criminal offence framework that obliges online corporations to delete or stop the spreading of degrading, offensive and humiliating content; also asks to put in place psychological support for women victims of online violence and girls who have been cyberbullied;

20. Stresses that illegal online content should be removed immediately by due legal process; highlights the role of information and communications technology, internet service providers and internet host providers in ensuring the fast and efficient removal of illegal online content at the request of the responsible law enforcement authority;

Prevention

21. Calls on the Commission, in the context of the review of the European cybersecurity strategy, to continue identifying network and information security vulnerabilities of European critical infrastructure, to incentivise the development of resilient systems, and to assess the situation regarding the fight against cybercrime in the EU and the Member States, in order to achieve a better understanding of trends and developments in relation to offences in cyberspace;

22. Stresses that cyber-resilience is key in preventing cybercrime and should therefore be given the highest priority; calls on Member States to adopt proactive policies and actions towards the defence of networks and critical infrastructure, calls for a comprehensive European approach to the fight against cybercrime that is compatible with fundamental rights, data protection, cybersecurity, consumer protection and e-commerce;

23. Welcomes, in this regard, the investment of EU funds in research projects such as the Cybersecurity public-private partnership (Cybersecurity PPP), aimed at fostering European cyber-resilience through innovation and capacity-building; recognises particularly the efforts made by the Cybersecurity PPP to develop appropriate responses to handling zero-day vulnerabilities;

24. Stresses, in this regard, the importance of free and open-source software; calls for more EU funds to be made available specifically for free and open-source software- based research into IT security;

25. Notes with concern that there is a lack of qualified IT professionals working on cybersecurity; urges Member States to invest in education;

26. Considers that regulation should play a greater role in managing cybersecurity risks

through improved product and software standards on design and subsequent updates, as well as minimum standards on default usernames and passwords;

27. Urges the Member States to step up information exchanges through Eurojust, Europol and ENISA, as well as best practice sharing through the European Network of CSIRT (Cyber Security Incident Response Teams) and CERTs (Computer Emergency Response Teams) on the challenges they face in the fight against cybercrime, as well as on concrete legal and technical solutions to address them and increase cyber-resilience; in this regard, calls on the Commission to promote effective cooperation and facilitate the exchange of information with a view to anticipating and managing potential risks, as provided for in the NIS Directive;

28. Is concerned by the Europol finding that the majority of successful attacks on individuals are attributable to a lack of digital hygiene and user awareness, or to insufficient attention being paid to technical security measures such as security by design; underlines that users are the first victims of badly secured hardware and software;

29. Calls on the Commission and the Member States to launch an awareness campaign, involving all relevant actors and stakeholders, to empower children and support parents, caretakers and educators in understanding and handling online risks and protecting children's safety online, to support Member States in setting up online sexual abuse prevention programmes, to promote awareness-raising campaigns on responsible behaviour in social media, and to encourage major search engines and social media networks to take a proactive approach to protecting child safety online;

30. Calls on the Commission and the Member States to launch awareness-raising information and prevention campaigns and to promote good practices in order to ensure that citizens, in particular children and other vulnerable users, but also central and local governments, vital operators and private-sector actors, especially SMEs, are aware of the risks posed by cybercrime, know how to be safe online and know how to protect their devices; calls further on the Commission and Member States to promote practical security measures such as encryption or other security and privacy-enhancing technologies and anonymisation tools;

31. Stresses that awareness-raising campaigns should be accompanied by educational programmes on the 'informed use' of information technology instruments; encourages Member States to include cybersecurity, as well as the risks and consequences of online personal data use, in schools' computing education curricula; underlines in this context the efforts made in the framework of the European strategy for an internet better suited to children (Better Internet for Kids (BIK) Strategy 2012);

32. Stresses the urgent need for the fight against cybercrime to include more efforts on education and training in network and information security (NIS), education and training, by introducing training on NIS, on secure software development and on personal data protection for computer science students, as well as basic NIS training for staff working in public administrations;

33. Considers that insurance against cyber-hacking could be one of the tools spurring action on security, both by companies made liable for software design and by users prompted

to use software properly;

34. Stresses that businesses should identify vulnerabilities and risks through regular assessments, protect their products and services by fixing vulnerabilities immediately, including through patch management policies and data protection updates, mitigate the effect of ransomware attacks by setting up robust backup regimes, and consistently report cyber-attacks;

35. Urges the Member States to set up CERTs to which businesses and consumers can report malicious emails and websites as foreseen by the NIS Directive, so that Member States are regularly informed of security incidents and measures to combat and mitigate the risk to their own systems; encourages Member States to consider establishing a database to record all types of cybercrime and to monitor the evolution of the relevant phenomena;

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

Enhancing the responsibility and liability of service providers

37. Considers enhanced cooperation between competent authorities and service providers to be a key factor in accelerating and streamlining mutual legal assistance and mutual recognition procedures. within the remits provided for by the European legal framework; calls on providers of electronic communications services not established in the Union to designate in writing representatives in the Union;

38. Reiterates that with respect to the Internet of Things (IoT), producers are the key starting-point for tightening up liability regimes which will lead to a better quality of products and a more secure environment in terms of external access and a documented update facility;

39. Believes that in view of innovation trends and the growing accessibility of IoT devices, particular attention must be paid to the security of all and even the simplest of devices; considers that it is in the interest of hardware producers and developers of innovative software to invest in solutions to prevent cybercrime and to exchange information on cybersecurity threats; urges the Commission and the Member States to promote the security by design approach, and urges the industry to include security by design solutions in all such devices; in this context, encourages the private sector to implement voluntary measures developed on the basis of relevant EU legislation such as the NIS Directive and aligned with internationally recognised standards in order to bolster trust in the security of software and devices, such as the IoT trust label;

40. Encourages service providers to subscribe to the Code of Conduct on Countering Illegal Hate Speech Online, and calls on the Commission and participating companies to continue cooperation on this issue;

41. Recalls that Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular

electronic commerce, in the Internal Market (the e-Commerce Directive)[1] exempts intermediaries from liability for content only if they play a neutral and passive role in relation to the transmitted and/or hosted content, but also requires an expeditious reaction to remove or disable access to content when an intermediary has actual knowledge of infringement or illegal activity or information;

42. Underlines the absolute need to protect law enforcement databases from security incidents and unlawful access, since this is a matter of concern for individuals; expresses concern regarding extraterritorial reach by law enforcement authorities in accessing data in the context of criminal investigations, and underlines the need to implement strong rules on the matter;

43. Believes that issues related to illegal on-line activity must be tackled in an expeditious and efficient manner, including through takedown procedures if the content is not or no longer needed for detection, investigation and prosecution; reminds that Member States may, when removal is not feasible, take necessary and proportionate measures to block access from Union territory to such content; stresses that such measures must comply with existing legislative and judicial procedures, as well as with the Charter, and must also be subject to adequate safeguards, including the possibility of judicial redress;

44. Highlights the role of digital information society service providers in ensuring the fast and efficient removal of illegal online content at the request of the responsible law enforcement authority, and welcomes the progress achieved in this regard, including through the contribution of the EU Internet Forum; stresses the need for stronger commitment and cooperation on the part of competent authorities and information society service providers to achieve quick and effective takedowns by the industry and avoid blocking illegal content through government measures; calls on the Member States to hold non-compliant platforms legally responsible; reiterates that any measures for removing illegal online content which stipulate terms and conditions should only be permitted if national procedural rules provide users with the option of asserting their rights before a court after learning of such measures;

45. Highlights that, in line with Parliament's resolution of 19 January 2016, 'Toward a Digital Single Market Act'[2], the limited liability of intermediaries is essential to the protection of the openness of the internet, fundamental rights, legal certainty and innovation; welcomes the Commission's intention to provide guidance on notice-and-takedown procedures, to assist online platforms in complying with their responsibilities and the rules on liability defined by the e-commerce Directive (2000/31/EC), to enhance legal certainty, and to increase user confidence; urges the Commission to come forward with a legislative proposal on the matter;

46. Calls for the application of the 'follow the money' approach, as outlined in Parliament's resolution of 9 June 2015 entitled 'Towards a renewed consensus on the enforcement of Intellectual Property Rights: An EU Action Plan'[3], based on the regulatory framework of the e-Commerce directive and the IPRED directive;

[1] OJ L 178, 17.7.2000, p. 1.
[2] Texts adopted, P8_TA(2016)0009.
[3] Texts adopted, P8_TA(2015)0220.

47. Underlines the crucial importance of providing continued and specific training and psychological support to content moderators in private and public entities that are responsible for assessing objectionable or illegal content online, as they should be considered the first responders in this field;

48. Calls on service providers to make provision for clear types of referrals and to set up a properly defined back-office infrastructure which makes it possible to act quickly and appropriately on referrals;

49. Calls on service providers to step up their efforts to raise awareness of the risks inherent in going online, in particular for children, by developing interactive tools and information materials;

Strengthening police and judicial cooperation

50. Is concerned that a considerable number of cybercrimes remain unpunished; deplores the fact that the use by internet service providers of technologies such as NAT CGN seriously hampers investigations by making it technically impossible to identify who exactly is using an IP address and thus who is responsible for online crimes; emphasises 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; stresses that judicial and law enforcement authorities have to be provided with sufficient capabilities to conduct legitimate investigations;

51. Urges the Member States 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'; stresses that feasible solutions must be offered, via both legislation and continuous technological evolution, where finding them is imperative for justice and security; calls on the Member States to cooperate, in consultation with the judiciary and Eurojust, in aligning the conditions for the lawful use of investigative tools online;

52. Stresses that 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; calls on all Member States to make use of the possibilities of lawful interception targeting suspected individuals, to establish clear rules regarding the prior judicial authorisation process for lawful interception 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 hacking activities;

53. Encourages the Member States to engage with the ICT security community and to encourage it to take a more active role in 'white hat' hacking and the reporting of illegal content, such as child sex abuse material;

54. Encourages Europol to establish an anonymous system for reporting from within hidden networks, which will allow individuals to report illegal content, such as depictions of child sex abuse material, to the authorities, using technical safeguards similar to those implemented by numerous press organisations which use such systems to facilitate the

exchange of sensitive data with journalists in a way that permits a greater degree of anonymity and security than is afforded by conventional email;

55. 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;

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

57. 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 cybercrime;

58. Emphasises the need to develop the practical basis for a common EU approach to the issue of jurisdiction in cyberspace, as pointed out at the informal meeting of justice and home affairs ministers held on 26 January 2016;

59. Stresses, in this regard, the need to develop shared procedural standards which can determine the territorial factors that provide grounds for the applicable law in cyberspace, and to define investigative measures which can be used regardless of geographic borders;

60. Recognises that such a common European approach, which needs to respect fundamental rights and privacy, will build trust among stakeholders, reduce the treatment delays of cross-border requests, establish interoperability among heterogeneous actors, and provide the opportunity to incorporate due process requirements in operational frameworks;

61. Believes that, in the long term, shared procedural standards on enforcement jurisdiction in cyberspace should also be developed at global level; welcomes, in this regard, the work of the Cloud Evidence Group of the Council of Europe;

e-Evidence

62. 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, as well as contributing to making the settlement of cases much speedier than today;

63. Underlines 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, including through the increased use of joint investigation teams, third countries and service providers active on European territory, in accordance with the GDPR (2016/679/EU), Directive 2016/680/EU of 27 April 2016 (the Police Directive)[1] and existing mutual legal assistance (MLA) agreements; stresses the need to set up single contact points within all Member States and to optimise the use of existing contact points, as this will

[1] OJ L 119, 4.5.2016, p. 89.

facilitate access to e-evidence as well as information-sharing, improve cooperation with service providers, and accelerate MLA proceedings;

64. Recognises that the currently fragmented legal framework can create challenges for service providers seeking to comply with law enforcement requests; 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 other Member States that are based on due legal process and in line with the European Investigation Order (EIO), while taking account of the principle of proportionality to avoid adverse effects on the exercise of the freedom of establishment and the freedom to provide services and ensuring adequate safeguards, with a view to establishing legal certainty as well as improving the ability of service providers and intermediaries to respond to law enforcement requests;

65. Stresses the need for any e-evidence framework to include sufficient safeguards for the rights and freedoms of all concerned; highlights that this should include a requirement that requests for e-evidence be directed in the first instance to the controllers or owners of the data, in order to ensure respect for their rights, as well as the rights of those to whom the data relates (for example their entitlement to assert legal privilege and to seek legal redress in the case of disproportionate or otherwise unlawful access); also highlights the need to ensure that any legal framework protects providers and all other parties from requests that could create conflicts of law or otherwise impinge on the sovereignty of other states;

66. Calls on the Member States to implement fully Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (the EIO Directive)[1] 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 allow judges to be issued clearer guidance regarding the penalisation of cybercrime;

67. Welcomes the ongoing work of the Commission towards a cooperation platform with a secure communication channel for digital exchanges of EIOs for e-evidence and replies between EU judicial authorities; invites the Commission, in association with Member States, Eurojust and service providers, to examine and align the forms, tools and procedures for requesting the securing and obtainment of e-evidence with a view to facilitating authentication, ensuring swift procedures and increasing the transparency and accountability of the process of securing and obtaining e-evidence; calls on the European Union Agency for Law Enforcement Training (CEPOL) to develop training modules on the effective use of current frameworks used to secure and obtain electronic evidence; stresses, in this context, that streamlining service providers' policies will help reduce the heterogeneity of approaches, notably regarding procedures and conditions for granting access to the requested data;

Capacity-building at European level

[1] OJ L 130, 1.5.2014, p. 1.

68. Points out that recent incidents have clearly demonstrated the acute vulnerability of the EU, and in particular the EU institutions, national governments and parliaments, major European companies, European IT infrastructures and networks, to sophisticated attacks using complex software and malware; calls on the European Union Agency for Network and Information Security (ENISA) to continuously evaluate the threat level, and on 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 EU's vulnerability to serious cyberattacks originating from large criminal organisations, state-sponsored attacks or terrorist groups;

69. Recognises the important contribution of the European Cybercrime Centre (EC3) of Europol and Eurojust, as well as of ENISA, to the fight against cybercrime;

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

71. Deplores the fact that currently no EU standards for training and certification exist; acknowledges that future trends in cybercrime require an increasing level of expertise from practitioners; welcomes the fact that existing initiatives such as the European Cybercrime Training and Education Group (ECTEG), the Training of Trainers (TOT) Project and the training activities under the EU Policy Cycle framework are already paving the way towards addressing the expertise gap at EU level;

72. Calls on 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;

73. Underlines that the number of cybercrime offences referred to Eurojust has increased by 30 %; calls for sufficient funding to be allocated, with more posts created if necessary, to enable Eurojust to cope with its increasing cybercrime-related workload, as well as to develop and strengthen further its support for national cybercrime prosecutors in cross-border cases, including via the recently established European Judicial Cybercrime Network;

74. Asks for a revision of ENISA's mandate and the reinforcement of the national cybersecurity agencies; calls for ENISA to be reinforced in terms of its tasks, staff and resources; stresses that the new mandate should also include stronger links with Europol and industry stakeholders, to allow the agency to better support the competent authorities in the fight against cybercrime;

75. Asks the Fundamental Rights Agency (FRA) to draw up a practical and detailed handbook providing guidelines regarding supervisory and scrutiny controls for Member States;

Improved cooperation with third countries

76. 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;

77. Calls on the Member States that have not yet done so to ratify and fully implement the Council of Europe Convention on Cybercrime of 23 November 2001 (the Budapest Convention), as well as its additional protocols, and, in cooperation with the Commission, to promote it in the appropriate international fora;

78. Stresses its serious concern regarding the work being done within the Council of Europe's Cybercrime Convention Committee on the interpretation of Article 32 of the Budapest Convention on transborder access to stored computer data (‘cloud evidence’), and opposes any conclusion of an additional protocol or guidance intended to broaden the scope of this provision beyond the current regime established by this Convention, which is already a major exception to the principle of territoriality because it could result in unfettered remote access for law enforcement authorities to servers and computers located in other jurisdictions without recourse to MLAs or other instruments of judicial cooperation put in place to guarantee the fundamental rights of the individual, including data protection and due process, including in particular Council of Europe Convention 108;

79. Regrets the fact that there is no binding international law on cybercrime, and urges the Member States and the European institutions to work towards establishing a convention on the matter;

80. Calls on the Commission to propose options for initiatives to improve the efficiency and promote the use of Mutual Legal Assistance Treaties (MLATs) in order to counter the assumption of extraterritorial jurisdiction by third countries;

81. Calls on the Member States to ensure sufficient capacity for handling MLA requests related to investigations in cyberspace, and to develop relevant training programmes for the staff responsible for handling such requests;

82. Underlines that strategic and operational cooperation agreements between Europol and third countries facilitate both the exchange of information and practical cooperation;

83. Takes note of the fact that the highest number of law enforcement requests are sent to the US and Canada; is concerned that the disclosure rate of big US service providers in response to requests from European criminal justice authorities falls short of 60 %, and recalls that according to Chapter V of the GDPR, MLATs and other international agreements are the preferred mechanism to enable access to personal data held overseas;

84. Calls on the Commission to put forward concrete measures to protect the fundamental rights of the suspected or accused person when exchange of information between European law enforcement authorities and third countries takes place, notably safeguards as regards the quick obtaining, upon a court decision, of relevant evidence, subscriber-related information or detailed metadata and content data (if not encrypted) from law-enforcement authorities and/or service providers, with a view to improving mutual legal assistance;

85. Calls on the Commission, in cooperation with Member States, the associated European bodies and, where necessary, third countries, to consider new ways to efficiently secure and obtain e-evidence hosted in third countries, in full compliance with fundamental rights and EU data protection law, by accelerating and streamlining the use of MLA

proceedings, and where applicable, mutual recognition;

86. Highlights the importance of the NATO Cyber Incidents Response Centre;

87. Calls on all Member States to participate in the Global Forum on Cyber Expertise (GFCE) in order to facilitate the establishment of partnerships to build capacity;

88. Supports the capacity-building assistance provided by the EU to the Eastern Neighbourhood countries, given that many cyberattacks originate in those countries;

°

° °

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

13.6.2017

OPINION OF THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION

for the Committee on Civil Liberties, Justice and Home Affairs

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

Rapporteur: Anneleen Van Bossuyt

AMENDMENTS

The Committee on the Internal Market and Consumer Protection calls on the Committee on Civil Liberties, Justice and Home Affairs, as the committee responsible, to take into account the following amendments:

Amendment 1
Motion for a resolution
Recital A a (new)

Motion for a resolution	*Amendment*
	Aa. whereas building confidence and trust in the online world is crucial to the creation and success of the Digital Single Market;

Amendment 2
Motion for a resolution
Recital A b (new)

Motion for a resolution	*Amendment*
	Ab. whereas an effective legal framework for data protection will at the same time allow consumers and businesses to fully reap the benefits of the

Digital Single Market and address cybercrime;

Amendment 3
Motion for a resolution
Recital I

Motion for a resolution	*Amendment*
I. whereas the constantly growing interconnectedness of people, places and things ***makes*** Internet of Things (IoT) devices an ideal target for cybercriminals;	I. whereas the constantly growing interconnectedness of people, places and things ***presents an increased risk of cybercrime as*** Internet of Things (IoT) devices ***are often not as well protected as traditional devices connected to the internet and as such are*** an ideal target for cybercriminals;

Amendment 4
Motion for a resolution
Paragraph 7 a (new)

Motion for a resolution	*Amendment*
	7a. Underlines that cybercrime severely undermines the functioning of the Digital Single Market in reducing trust in digital service providers, undermining cross-border transactions and seriously harming the interests of consumers of digital services;

Amendment 5
Motion for a resolution
Paragraph 11

Motion for a resolution	*Amendment*
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;	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; ***calls on the Commission, in this regard, to promote effective cooperation and facilitate information exchange between***

competent authorities with a view to anticipating and managing potential risks, as provided for in the NIS Directive;

Amendment 6
Motion for a resolution
Paragraph 13

Motion for a resolution	*Amendment*
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;	13. Calls on the Commission and the Member States to launch awareness-raising campaigns to ensure that citizens, in particular children ***minors*** 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;

Amendment 7
Motion for a resolution
Paragraph 16

Motion for a resolution	*Amendment*
16. Considers enhanced cooperation ***with*** service providers to be a key factor in accelerating and streamlining mutual legal assistance and mutual recognition procedures;	16. Considers enhanced cooperation ***between competent authorities and*** service providers to be a key factor in accelerating and streamlining mutual legal assistance and mutual recognition procedures;

Amendment 8
Motion for a resolution
Paragraph 16 a (new)

Motion for a resolution	*Amendment*
	16a. Considers that EU and national authorities should have the power to adopt interim measures to prevent the risk of serious and irreparable harm to consumers, in particular the suspension of a website, domain or a similar digital site, service or account, provided that the fundamental rights of EU citizens, rules

	on data protection and national law are respected;

Amendment 9
Motion for a resolution
Paragraph 17

Motion for a resolution	*Amendment*
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;	17. Believes that ***it is in the interests of developers of innovative*** software and ***of*** hardware producers ***to invest in solutions to prevent cybercrime;*** encourages the private sector***, in this context,*** to implement voluntary measures***, such as standards*** aimed at bolstering trust in the security of software and devices, such as the IoT trust label***, developed on the basis of relevant EU legislation such as the NIS Directive***;

Amendment 10
Motion for a resolution
Paragraph 18

Motion for a resolution	*Amendment*
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;***	***deleted***

Amendment 11
Motion for a resolution
Paragraph 19

Motion for a resolution	*Amendment*
19. Calls on the Commission to investigate ***the legal scope*** for improving the accountability of service providers and	19. Calls on the Commission to investigate ***options*** for improving the accountability of service providers and

for imposing an obligation to respond to foreign EU law-enforcement requests;	***intermediaries and the legal scope*** for imposing an obligation to respond to foreign EU law-enforcement requests***, taking into account the principle of proportionality, in order to avoid introducing measures liable to hinder or make less attractive the exercise of the freedom of establishment and the freedom to provide services***;

Amendment 12
Motion for a resolution
Paragraph 19 a (new)

Motion for a resolution	*Amendment*
	19a. Believes that guidance is needed from the Commission on the implementation of the intermediary liability framework in order to allow online platforms to comply with their responsibilities and the rules on liability, to enhance legal certainty, and to increase user confidence; calls on the Commission to take further steps to that effect, and recalls that the e-Commerce Directive exempts intermediaries from liability for content only if they play a neutral and passive role in relation to the transmitted and/or hosted content but requires as well an expeditious reaction to remove or disable access to content when an intermediary has actual knowledge of infringement or illegal activity or information;

Amendment 13
Motion for a resolution
Paragraph 20

Motion for a resolution	*Amendment*
20. ***Calls on the Member States to impose the same encryption obligations on online service providers as those, which apply to providers of traditional***	***deleted***

telecommunications services;

Amendment 14
Motion for a resolution
Paragraph 21

Motion for a resolution	*Amendment*
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;	21. ***Believes that issues related to*** illegal online content ***must be tackled in an efficient manner, including by restricting access to online content or through takedown procedures***; 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 ***competent authorities and digital*** service providers to respond quickly and effectively;

Amendment 15
Motion for a resolution
Paragraph 21 a (new)

Motion for a resolution	*Amendment*
	21 a. Calls for the 'follow the money' approach to be applied, as outlined in its resolution of 9 June 2015 on 'Towards a renewed consensus on the enforcement of Intellectual Property Rights: An EU Action Plan'[1], based on the regulatory framework of the E-Commerce Directive and the Intellectual Property Rights Enforcement Directive;
	[1] OJ C 407, 4.11.2016, p. 25.

Amendment 16
Motion for a resolution
Paragraph 21 b (new)

Motion for a resolution	*Amendment*
	21b. Stresses that, as stated in its resolution of 19 January 2016 on 'Towards a Digital Single Market Act'[1], the limited liability of intermediaries is essential to the protection of the openness of the internet, fundamental rights, legal certainty and innovation; welcomes the Commission's intention to provide guidance to assist online platforms in complying with the e-Commerce Directive; calls on the Commission to take further steps to that effect, recalling that platforms not playing a neutral role as defined in the e-Commerce Directive cannot claim liability exemption;
	[1] Texts adopted, P8_TA(2016)0009.

INFORMATION ON ADOPTION IN COMMITTEE ASKED FOR OPINION

Date adopted	8.6.2017
Result of final vote	+: 0 –: 0 0: 0

INFORMATION ON ADOPTION IN COMMITTEE RESPONSIBLE

Date adopted	11.7.2017
Result of final vote	+: 50 –: 4 0: 2
Members present for the final vote	Jan Philipp Albrecht, Gerard Batten, Malin Björk, Michał Boni, Caterina Chinnici, Agustín Díaz de Mera García Consuegra, Frank Engel, Tanja Fajon, Raymond Finch, Monika Flašíková Beňová, Kinga Gál, Ana Gomes, Nathalie Griesbeck, Sylvie Guillaume, Jussi Halla-aho, Sophia in ‘t Veld, Dietmar Köster, Barbara Kudrycka, Cécile Kashetu Kyenge, Marju Lauristin, Juan Fernando López Aguilar, Monica Macovei, Roberta Metsola, Claude Moraes, Soraya Post, Judith Sargentini, Birgit Sippel, Branislav Škripek, Csaba Sógor, Traian Ungureanu, Bodil Valero, Kristina Winberg, Tomáš Zdechovský, Auke Zijlstra
Substitutes present for the final vote	Kostas Chrysogonos, Carlos Coelho, Pál Csáky, Anna Hedh, Marek Jurek, Miltiadis Kyrkos, Jean Lambert, Jeroen Lenaers, Morten Helveg Petersen, John Procter, Christine Revault D’Allonnes Bonnefoy, Petri Sarvamaa, Barbara Spinelli, Jaromír Štětina, Axel Voss, Elissavet Vozemberg-Vrionidi
Substitutes under Rule 200(2) present for the final vote	Beatriz Becerra Basterrechea, Izaskun Bilbao Barandica, André Elissen, Arne Gericke, Josu Juaristi Abaunz, Georg Mayer

FINAL VOTE BY ROLL CALL IN COMMITTEE RESPONSIBLE

50	+
ALDE	Beatriz Becerra Basterrechea, Izaskun Bilbao Barandica, Nathalie Griesbeck, Morten Helveg Petersen, Sophia in 't Veld
ECR	Arne Gericke, Jussi Halla-aho, Marek Jurek, Monica Macovei, John Procter, Branislav Škripek
GUE/NGL	Malin Björk, Kostas Chrysogonos, Josu Juaristi Abaunz, Barbara Spinelli
PPE	Michał Boni, Carlos Coelho, Pál Csáky, Agustín Díaz de Mera García Consuegra, Frank Engel, Kinga Gál, Barbara Kudrycka, Jeroen Lenaers, Roberta Metsola, Petri Sarvamaa, Jaromír Štětina, Csaba Sógor, Traian Ungureanu, Axel Voss, Elissavet Vozemberg-Vrionidi, Tomáš Zdechovský
S&D	Caterina Chinnici, Tanja Fajon, Monika Flašíková Beňová, Ana Gomes, Sylvie Guillaume, Anna Hedh, Cécile Kashetu Kyenge, Miltiadis Kyrkos, Dietmar Köster, Marju Lauristin, Juan Fernando López Aguilar, Claude Moraes, Soraya Post, Christine Revault D'Allonnes Bonnefoy, Birgit Sippel
VERTS/ALE	Jan Philipp Albrecht, Jean Lambert, Judith Sargentini, Bodil Valero

4	-
EFDD	Gerard Batten, Raymond Finch
ENF	André Elissen, Auke Zijlstra

2	0
EFDD	Kristina Winberg
ENF	Georg Mayer

Key to symbols:
+ : in favour
- : against
0 : abstention