EUROPEAN PARLIAMENT 2009 - 2014

Plenary sitting

A7-0224/2013

18.6.2013

***I
REPORT

on the proposal for a directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA
(COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Monika Hohlmeier

PR_COD_1amCom

Symbols for procedures

*	Consultation procedure
***	Consent procedure
***I	Ordinary legislative procedure (first reading)
***II	Ordinary legislative procedure (second reading)
***III	Ordinary legislative procedure (third reading)

(The type of procedure depends on the legal basis proposed by the draft act.)

Amendments to a draft act

In amendments by Parliament, amendments to draft acts are highlighted in ***bold italics***. Highlighting in *normal italics* is an indication for the relevant departments showing parts of the draft act which may require correction when the final text is prepared – for instance, obvious errors or omissions in a language version. Suggested corrections of this kind are subject to the agreement of the departments concerned.

The heading for any amendment to an existing act that the draft act seeks to amend includes a third line identifying the existing act and a fourth line identifying the provision in that act that Parliament wishes to amend. Passages in an existing act that Parliament wishes to amend, but that the draft act has left unchanged, are highlighted in **bold**. Any deletions that Parliament wishes to make in such passages are indicated thus: **[...]**.

CONTENTS

Page

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

on the proposal for a directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

(Ordinary legislative procedure: first reading)

The European Parliament,

– having regard to the Commission proposal to Parliament and the Council (COM(2010)0517),

– having regard to Article 294(2) and Article 83(1) of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C7-0293/2010),

– having regard to Article 294(3) of the Treaty on the Functioning of the European Union,

– having regard to the opinion of the European Economic and Social Committee of 4 May 2011[1],

– having regard to the undertaking given by the Council representative by letter of xxx to approve Parliament's position, in accordance with Article 294(4) of the Treaty on the Functioning of the European Union,

– having regard to Rule 55 of its Rules of Procedure,

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs and the opinions of the Committee on Foreign Affairs and the Committee on Industry, Research and Energy (A7-0224/2013),

1. Adopts its position at first reading hereinafter set out;

2. Calls on the Commission to refer the matter to Parliament again if it intends to amend its proposal substantially or replace it with another text;

3. Instructs its President to forward its position to the Council, the Commission and the national parliaments.

Amendment 129
Proposal for a directive
–

[1] OJ C 218, 23.7.2011, p. 130.

AMENDMENTS BY THE EUROPEAN PARLIAMENT*

to the Commission proposal

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on attacks against information systems and *replacing* Council Framework Decision 2005/222/JHA

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 83(1) thereof,

Having regard to the proposal from the European Commission[1],

After transmission of the draft legislative act to the national Parliaments,

Having regard to the opinion of the European Economic and Social Committee[2],

Having regard to the opinion of the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure,

---

* Amendments: new or amended text is highlighted in bold italics; deletions are indicated by the symbol ▌.

1 OJ C […], […], p. […].

2 ***OJ C […], […], p. […].***

Whereas:

(1) The objective of this Directive is to approximate ***the criminal legislation*** in the Member States in the area of attacks against information systems, ***by establishing minimum rules concerning the definition of criminal offences and the sanctions in this area, and to*** improve cooperation between ▌ competent authorities, including the police and other specialised law enforcement services of the Member States***, as well as the competent specialised agencies of the Union, such as Eurojust, Europol and its European Cyber Crime Centre, and the European Network and Information Security Agency (ENISA).***

(1a) Information systems are a key element of political, social and economic interaction in the Union. Society is highly and increasingly dependent on such systems. The smooth operation and security of these systems in the Union is vital for the development of the internal market and of a competitive and innovative economy. Ensuring appropriate levels of protection of information systems should form part of an effective comprehensive framework of prevention measures accompanying criminal law responses to cybercrime.

(2) Attacks against information systems, in particular ***attacks linked to*** organised crime, are a growing menace ***both in the EU and globally***, and there is increasing concern about the potential for terrorist or politically motivated attacks against information systems which form part of the critical infrastructure of Member States and the Union. This constitutes a threat to the achievement of a safer information society and an area of freedom, security***,*** and justice, and therefore requires a response at the level of the European Union ***and improved cooperation and coordination at international level***.

(2a) There are a certain number of critical infrastructures in the Union, the disruption or destruction of which would have significant cross-border impacts. It emerges from the need to increase the critical infrastructure protection capability in the Union that the measures against cyber attacks should be complemented by serious criminal penalties reflecting the gravity of such attacks. Critical infrastructure may be understood as an asset, system or part thereof located in Member States which is essential for instance for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, such as power plants, transport networks or government networks and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

(3) There is evidence of a tendency towards increasingly dangerous and recurrent large scale attacks conducted against information systems which ***often can be*** critical to states or to particular functions in the public or private sector. This tendency is accompanied by the development of increasingly sophisticated ***methods, such as the creation and use of the so called "botnets", which involves subsequent stages of the criminal act, where each stage alone could pose serious danger to public interests. In this respect, the Directive aims, inter alia, to introduce criminal sanctions for the stage where the "botnet" is created, namely, where remote control over a significant number of computers is established by infecting them with malicious software, through targeted cyber attacks. At a later stage, the infected network of computers, constituting the "botnet", could be activated without the computer users' knowledge in order to launch a large scale cyber attack, which usually would have the capacity to cause serious damage, as referred to in this Directive. Member States may determine what constitutes serious damage according to their national law and practice, which may include disrupted system services of significant public importance, or major financial cost or loss of personal data or sensitive information.***

(3a) Large scale attacks can cause substantial economic damage both through interruption of information systems and communications and through loss or alteration of commercially important confidential information or other data. Particular attention should be paid to raising the awareness of innovative SMEs of related threats and vulnerabilities, due to their increased dependence on the proper functioning and availability of information systems and often limited resources for information security.

(4) Common definitions in this area are important in order to ensure a consistent approach in the Member States to the application of this Directive.

(5) There is a need to achieve a common approach to the constituent elements of criminal offences by introducing common offences of illegal access to an information system, illegal system interference, illegal data interference, and illegal interception.

(5a) Interception includes, but is not necessarily limited to the listening to, monitoring or surveillance of the content of communications and the procuring of the content of data either directly, through access and use of the information systems, or indirectly through the use of electronic eavesdropping or tapping devices by technical means.

(6) Member States should provide for penalties in respect of attacks against information systems. The penalties provided for should be effective, proportionate and dissuasive ***and should include imprisonment and/or financial penalties.***

(6a) The directive provides for criminal sanctions at least for cases which are not minor. Member States may determine what constitutes a minor case according to their national law and practice. The case may be considered minor, for example, when the damage caused by the offence and/or the risk it carries to public or private interests, such as to the integrity of a computer system or computer data, or to a person's integrity, rights and other interests, is insignificant or is of such nature, that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary.

(6b) The identification and reporting of threats and risks posed by cyber attacks, as well as related vulnerabilities of information systems is a pertinent element of an effective prevention and response to cyber attacks and of improving the security of information systems. Providing incentives to report security gaps could add to that effect. Member States should endeavour to provide possibilities, so as to allow the legal detection and reporting of security gaps.

(7) It is appropriate to provide for more severe penalties when an attack against an information system is committed by a criminal organisation, as defined in Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime[1] ***or*** when the attack is conducted on a large scale, ***thus affecting a significant number of information systems or causing serious damage, including when the attack is intended to create a "botnet" or is carried out through a "botnet", thus resulting in serious damage***. It is also appropriate to provide for more severe penalties where such an attack ***is conducted against a critical infrastructure.***

(7a) Setting up effective measures against identity theft and other identity related offences constitutes another important element of an integrated approach against Cybercrime. Any need for EU action regarding this type of criminal behaviour could be also considered in the context of evaluating the necessity for a comprehensive horizontal EU instrument.

(8) The Council Conclusions of 27-28 November 2008 indicated that a new strategy should be developed with the Member States and the Commission, taking into account the content of the 2001 Council of Europe Convention on Cybercrime. That Convention is the legal framework of reference for combating cybercrime, including attacks against information systems. This Directive builds on that Convention. ***Completing the process of ratification of the Convention by all Member States as soon as possible should thus be considered a priority.***

[1] OJ L 300, 11.11.2008, p. 42.

(9) Given the different ways in which attacks can be conducted, and given the rapid developments in hardware and software, this Directive ***refers*** to 'tools' that can be used in order to commit the crimes listed in this Directive. Tools refer to, for example, malicious software, including ***those able to create*** botnets, used to commit cyber attacks. ***Even if a tool is suitable or even especially suitable for carrying out the mentioned offences the tool might be produced for legitimate purposes. Motivated by the need to avoid criminalisation where such tools are produced and put on the market for legitimate purposes, such as testing the reliability of information technology products or the security of information systems, apart from the general intent requirement, a direct intent requirement that those tools be used for the purposes of committing any of the offences referred to in the Directive must be also fulfilled.***

I

(10a) This Directive does not intend to impose criminal liability where the objective criteria of the crimes listed in this directive are met, but the acts are committed without criminal intent, for instance when the person did not know that the access was unauthorised or in the case of mandated testing or protection of information systems, e.g. when a person is assigned by a company or vendor to test the strength of its security system. In the context of this Directive, contractual obligations or agreements to restrict the access to information systems by way of user policy or terms of service, as well as labour disputes as regards the access to and use of information systems of the employer for private purposes, should not incur criminal liability, where the access under such circumstances would be deemed unauthorised and thus would constitute the sole basis for criminal proceeding. This Directive is without prejudice to the legally guaranteed right of access to information as laid down in national and EU legislation, while at the same time it may not serve as an exemption to justify unlawful and arbitrary access to information.

(10b) The commission of cyber attacks could be facilitated by various circumstances, such as when the perpetrator within the scope of his employment has access to the security systems inherent in the affected information systems. In the context of national law such circumstances should be appropriately taken into account in the course of criminal proceedings.

(10c) Member States should provide for aggravating circumstances in their national law in accordance with the applicable rules established by their legal systems on aggravating circumstances. They should ensure that those aggravating circumstances are available for judges to consider when sentencing offenders. It remains within the discretion of the judge to assess these circumstances together with the other factual elements of the particular case.

(10d) This Directive does not govern the conditions that should be met in order to exercise jurisdiction over any of the offences referred to in Art. 3 to 8, such as a report made by the victim in the place where the offence was commited, or a denunciation from the State of the place where the offence was commited, or the fact that the offender has not been prosecuted in the place where the offence was committed.

(10e) In the context of this Directive, States and public bodies remain fully bound to guarantee respect for human rights and fundamental freedoms, in accordance with existing international obligations.

(11) This Directive strengthens the importance of networks, such as the G8 or the Council of Europe's network of points of contact available on a twenty-four hour, seven-day-a-week basis***. Such points of contact should be able to deliver effective assitance thus facilitating for example the exchange of available relevant information or provision of technical advice or legal information*** for the purpose of investigations or proceedings concerning criminal offences ***relating*** to information systems and ***associated data involving the requesting Member State. In order to ensure the smooth operation of the networks each contact point should have the capacity to carry out communications with the point of contact of another Member State on an expedited basis supported inter alia by trained and equipped personnel***. Given the speed with which large-scale ***cyber*** attacks can be carried out, Member States should be able to respond promptly to urgent requests from this network of contact points. ***In such cases, it may be expedient that the request for information is accompanied by telephone contact, in order to ensure that the request is processed swiftly by the requested Member State and that feedback will be provided within 8 hours.***

(11a) Cooperation between the public authorities and the private sector and civil society is of great importance in preventing and combating attacks against information systems. It is necessary to foster and improve cooperation between service providers, producers, law enforcement bodies and judicial authorities, while fully respecting the rule of law. The cooperation may include, for example, support by service providers in helping to preserve potential evidence, in providing elements helping to identify perpetrators and, as a last resort, shutting down, completely or partially, in accordance with national law, including national legislation and practice, information systems or functions that have been compromised or used for illegal purposes. Member States should also consider setting up cooperation and partnership networks with service providers and producers for the exchange of information in relation to the offences within the scope of this Directive.

I

(12a) There is a need to collect comparable data on offences referred to in this Directive. Relevant data should be made available to the competent specialised agencies, such as Europol and the European Network and Information Security Agency in line with their tasks and information needs, in order to gain a more complete picture of the problem of cybercrime and network and information security at Union level and thereby contribute to formulating more effective responses. Member States should submit information on the modus operandi used by the perpetrators to Europol and its European Cybercrime Centre for the purpose of conducting threat assessments and strategic analyses of cybercrime in accordance with the Council Decision 2009/371/JHA. Providing information can facilitate a better understanding of present and future threats and thus contribute to a more appropriate and targeted decision-making on combating and preventing attacks against information systems.

(12b) In accordance with this Directive the Commission has to submit a report on the application of the Directive and to make any necessary legislative proposals possibly leading to broadening of the scope of this Directive taking into account developments in the field of Cybercrime. Such developments could include any technological developments enabling for example more effective enforcement in the area of attacks against information systems or which facilitate prevention or minimise the impact of such attacks. For this purpose the Commission should take into account the available analysis and reports produced by relevant actors and in particular Europol and ENISA.

(12c) In order to fight cybercrime effectively, it is necessary to increase the resilience of information systems by taking appropriate measures to protect them more effectively against Cyber attacks. Member States should take necessary measures to protect critical infrastructures from cyber attacks, as part of which they should consider the protection of their information systems and associated data. Ensuring an adequate level of protection and security of information systems by legal persons, for example in connection with the provision of publicly available electronic communications services in line with existing EU legislation on privacy and electronic communication and data protection, forms an essential part of a comprehensive approach to effectively counteracting cybercrime. Appropriate levels of protection should be provided against reasonably identifiable threats and vulnerabilities in accordance with the state of the art for specific sectors and the specific data processing situations. The cost and burden of such protection should be proportionate to the likely damage a cyber attack would cause to those affected. Member States are encouraged to provide for relevant measures incurring liabilities in the context of their national law in cases where a legal person has clearly not provided an appropriate level of protection against cyber attacks.

(13) Significant gaps and differences in Member States' laws ***and criminal procedures*** in the area of attacks against information systems ▌ may hamper the fight against organised crime and terrorism, and may complicate effective police and judicial cooperation in this area. The transnational and borderless nature of modern information systems means that attacks against such systems have a ***cross-border*** dimension, thus underlining the urgent need for further action to approximate criminal legislation in this area. Besides that, the coordination of prosecution of cases of attacks against information systems should be facilitated by the ***adequate implementation and application*** of Council Framework Decision 2009/948/JHA on prevention and settlement of conflict of jurisdiction in criminal proceedings. ***Member States in cooperation with the European Union should also seek to improve international cooperation related to security of information systems, computer networks and computer data. Proper consideration to the security of data transfer and storage should be given in any international agreement involving data exchange.***

(13a) Improved cooperation between the competent law enforcement bodies and judicial authorities across the Union is essential in an effective fight against cybercrime. In this context stepping up the efforts to provide adequate training to the relevant authorities in order to raise the understanding of cybercrime and its impact, and to foster cooperation and exchange of best practices, for example via the competent specialised EU agencies should be encouraged. Such training should aim inter alia at raising awareness about the different national legal systems, the possible legal and technical challenges faced in criminal investigations, or the distribution of competences between the relevant national authorities.

(14) Since the objectives of this Directive, i.e. ensuring that attacks against information systems are punished in all Member States by effective, proportionate and dissuasive criminal penalties and improving and encouraging judicial cooperation by removing potential complications, cannot be sufficiently achieved by the Member States, as rules have to be common and compatible, and can therefore be better achieved at the level of the Union, the Union may adopt measures in accordance with the principle of subsidarity as set out in Article 5 of the Treaty on European Union. This Directive does not go beyond what is necessary in order to achieve those objectives.

I

(15a) The protection of personal data is a fundamental right in accordance with Article 16 (1) TFEU and Article 8 of the Charter on Fundamental rights. Therefore, any processing of personal data in the context of the implementation of this Directive should fully comply with the relevant EU legislation on data protection adopted on the basis of the Treaties.

(16) This Directive respects the fundamental ***freedoms and*** rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union ***and the European Convention for the Protection of Human Rights and Fundamental Freedoms***, including the protection of personal data***, the right to privacy***, freedom of expression and information, the right to a fair trial, presumption of innocence and the rights of the defence, as well as the principles of legality and proportionality of criminal offences and penalties. In particular, this Directive seeks to ensure full respect for these rights and principles and must be implemented accordingly.

(17) ***In accordance with Article 3*** of the Protocol on the position of United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on the Functioning of the European Union, the United Kingdom and Ireland have notified their wish to participate in the adoption and application of this Directive ▌.

(18) In accordance with Articles 1 and 2 of Protocol on the position of Denmark annexed to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Directive and is therefore not bound by it or subject to its application**.**

(19) This Directive aims to amend and expand the provisions of Framework Decision 2005/222/JHA. Since the amendments to be made are of substantial number and nature, the Framework Decision should, in the interests of clarity, be replaced in its entirety in relation to Member States participating in the adoption of this Directive.

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Subject matter

I

This Directive establishes minimum rules concerning the definition of criminal offences and the sanctions in the area of attacks against information systems. It also aims to facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities.

Article 2

Definitions

For the purposes of this Directive, the following definitions shall apply:

(a) "information system" means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance;

(b) "computer data" means any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function;

(c) "legal person" means any entity having such status under the applicable law, except for States or other public bodies in the exercise of State authority and for public international organisations;

(d) "without right" means ***access***, ***interference, interception, or any other conduct referred to in this Directive,*** not authorised by the owner, other right holder of the system or of part of it, or not permitted under national legislation.

Article 3

Illegal access to information systems

Member States shall take the necessary measures to ensure that***, when committed intentionally, the*** access without right to the whole or any part of an information system is punishable as a criminal offence ***when the offence is committed by infringing a security measure***, at least for cases which are not minor.

Article 4

Illegal system interference

Member States shall take the necessary measures to ensure that the ▌ serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed ***intentionally and*** without right, at least for cases which are not minor.

Article 5

Illegal data interference

Member States shall take the necessary measures to ensure that the ▌ deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed ***intentionally and*** without right, at least for cases which are not minor.

Article 6

Illegal interception

Member States shall take the necessary measures to ensure that the ▌ interception by technical means, of non-public transmissions of computer data to, from or within a information system, including electromagnetic emissions from an information system carrying such computer data, is punishable as a criminal offence when committed ***intentionally and without right, at least for cases which are not minor***.

Article 7

Tools used for committing offences

1. Member States shall take the necessary ***measures*** to ensure that the production, sale, procurement for use, import, ▌ distribution or otherwise making available of the following is punishable as a criminal offence when committed intentionally and without right***, with the intent that it be used*** for the purpose of committing any of the offences referred to in Articles 3 to ***6, at least for cases which are not minor***:

(a) ▌ a computer program, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;

(b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.

Article 8

***Incitement**, aiding **and** abetting and attempt*

1. Member States shall ensure that the ***incitement***, aiding and abetting ***to commit*** an offence referred to in Articles 3 to 7 is punishable as a criminal offence.

2. Member States shall ensure that the attempt to commit ***an offence*** referred to in ***Articles 4 to 5*** is punishable as a criminal offence.

Article 9

Penalties

1. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 8 are punishable by effective, ***proportionate*** and dissuasive criminal penalties.

2. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 7 are punishable by ***a maximum penalty of at least two years of imprisonment, at least in cases which are not minor***.

3. Member States shall take the necessary measures to ensure that the offences referred to in Articles 4 to 5, when committed intentionally, are punishable by a maximum penalty of at least three years of imprisonment when a significant number of information systems have been affected through the use of a tool, referred to in Article 7 (1), designed or adapted primarily for this purpose.

4. Member States shall take the necessary measures to ensure that offences referred to in Articles 4 to 5 are punishable by a maximum penalty of at least five years of imprisonment when

(a) committed within the framework of a criminal organisation, as defined in Framework Decision 2008/814/JHA irrespective of the penalty level referred to therein, or

(b) causing serious damage, or

(c) committed against a critical infrastructure information system.

5. Member States shall take the necessary measures to ensure that when the offences referred to in Articles 4 and 5 are committed by misusing personal data of another person, with the aim of gaining trust of a third party, thereby causing prejudice to the rightful identity owner, this may, in accordance with relevant provisions of national law, be regarded as aggravating circumstances, unless these circumstances are already covered by another offence, punishable under the national legislation.

I

Article 11

Liability of legal persons

1. Member States shall take the necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 3 to 8, committed for their benefit by any person, acting either individually or as part of an organ of the legal person, and having a leading position within the legal person, based on one of the following:

(a) a power of representation of the legal person;

(b) an authority to take decisions on behalf of the legal person;

(c) an authority to exercise control within the legal person.

2. Member States shall take the necessary measures to ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission, by a person under its authority, of any of the offences referred to in Articles 3 to 8 for the benefit of that legal person.

3. Liability of legal persons under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are perpetrators of***, inciters***, or accessories to, any of the offences referred to in Articles 3 to 8.

Article 12

Penalties on legal persons

1. Member States shall take the necessary measures to ensure that a legal person held liable pursuant to Article 11(1) is punishable by effective, proportionate and dissuasive penalties, which shall include criminal or non-criminal fines and may include other sanctions, for example:

(a) exclusion from entitlement to public benefits or aid;

(b) temporary or permanent disqualification from the practice of commercial activities;

(c) placing under judicial supervision;

(d) judicial winding-up;

(e) temporary or permanent closure of establishments which have been used for committing the offence.

2. Member States shall take the necessary measures to ensure that a legal person held liable pursuant to Article 11(2) is punishable by effective, proportionate and dissuasive penalties or measures .

Article 13

Jurisdiction

1. Member States shall establish their jurisdiction with regard to the offences referred to in Articles 3 to 8 where the offence has been committed:

(a) in whole or in part within the territory of the Member State concerned; or

(aa) by one of their nationals, at least in cases when the act is a criminal offence at the place where it was performed.

I

2. When establishing jurisdiction in accordance with paragraph 1(a), ***a Member State*** shall ensure that the jurisdiction includes cases where:

(a) the offender commits the offence when physically present on the territory of the Member State concerned, whether or not the offence is against an information system on its territory; or

(b) the offence is against an information system on the territory of the Member State concerned, whether or not the offender commits the offence when physically present on its territory.

3. A Member State shall inform the Commission where it decides to establish further jurisdiction over an offence referred to in Articles 3 to 8 committed outside of their territory e.g. where:

(a) the offender has his or her habitual residence in the territory of that Member State; or

(b) the offence is committed for the benefit of a legal person established in the territory of that Member State.

Article 14

Exchange of information

1. For the purpose of exchange of information relating to the offences referred to in Articles 3 to 8, ***Member States shall ensure that they have an operational national point of contact and*** make use of the existing network of operational points of contact available 24 hours a day and seven days a week. Member States shall also ensure that they have procedures in place so that ***in urgent requests they can indicate within a maximum of 8 hours at least whether the request for help will be answered, as well as the form and the estimated time of this answer***.

2. Member States shall inform the Commission of their appointed point of contact for the purpose of exchanging information on the offences referred to in Articles 3 to 8. The Commission shall forward that information to the other Member States ***and competent specialised EU agencies and bodies***.

3. Member States shall take the necessary measures to ensure that appropriate reporting channels are made available in order to facilitate reporting without undue delay of the offences referred to in Article 3 to 6 to the competent national authorities.

Article 15

Monitoring and statistics

1. Member States shall ensure that a system is in place for the recording, production and provision of statistical data on the offences referred to in Articles 3 ***to 7.***

2. The statistical data referred to in paragraph 1 shall, as a minimum, cover ***existing data on*** the number of offences referred to in Articles 3 to ***7 registered by*** the Member States***,*** and ▌ the number of persons***, prosecuted and convicted*** for the offences referred to in Articles 3 ***to 7.***

3. Member States shall transmit the data collected according to this Article to the Commission. ***The Commission shall ensure*** that a consolidated review of these statistical reports is published ***and submitted to the competent specialised EU agencies and bodies***.

Article 16

Replacement *of Framework Decision 2005/222/JHA*

Framework Decision 2005/222/JHA is hereby ***replaced in relation to Member States participating in the adoption of this Directive***, without prejudice to the obligations of the Member States relating to the time ***limit*** for transposition ***of the Framework Decision*** into national law.

In relation to Member States participating in the adoption of this Directive, references to the Framework Decision ***2005/222/JHA*** shall be construed as references to this Directive.

Article 17

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by [two years from adoption] ▌.

▌

3. Member States shall transmit to the Commission the text of the provisions transposing into their national law the obligations imposed on them under this Directive.

4. When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

Article 18

Reporting

▌

The Commission shall by [FOUR YEARS FROM ADOPTION], submit a report to the European Parliament and the Council, assessing the extent to which the Member States have taken the necessary measures in order to comply with this Directive, accompanied, if necessary, by legislative proposals. In this respect, the Commission shall also take into account the technical and legal developments in the field of cyber crime, particularly with regard to the scope of this Directive.

▌

Article 19

Entry into force

This Directive shall enter into force on the twentieth day following its publication in the Official Journal of the European Union.

Article 20

Addressees

This Directive is addressed to the Member States in accordance with the Treaties.

28.11.2011

OPINION OF THE COMMITTEE ON FOREIGN AFFAIRS

for the Committee on Civil Liberties, Justice and Home Affairs

on the proposal for a directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

Rapporteur: Kristiina Ojuland

SHORT JUSTIFICATION

The opinion strongly supports the need for a better exchange of information related to cyber security among Member States, in the context of increasing concern about potential cyber attacks. There is a real urgency to address the issue of cyber security on the EU level and through coordinated actions of the Member States.

The opinion underlines the role of the Commission to facilitate the promotion and coordination of existing initiatives.

The Committee on Foreign Affairs and the Subcommittee on Security and Defence believe that the urgent need to act and reinforce the coordination of the responses, initiatives and programmes on EU level is of great importance. The development of capabilities and stronger collaboration to increase the level of information security should be supported.

The opinion supports the idea of the appointment of an EU Cyber Security Coordinator, in order to facilitate integration and coordination of different European activities and initiatives on the EU level and across EU institutions.

AMENDMENTS

The Committee on Foreign Affairs calls on the Committee on Civil Liberties, Justice and Home Affairs, as the committee responsible, to incorporate the following amendments in its report:

Amendment 1

Proposal for a directive
Recital 1

Text proposed by the Commission	*Amendment*
(1) The objective of this Directive is to approximate rules on criminal law in the Member States in the area of attacks against information systems, and improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States.	(1) The objective of this Directive is to approximate rules on criminal law in the Member States in the area of attacks against information systems, and improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States ***and of the Union. That this objective forms part of the Union's general strategy to combat organised crime, secure information networks more effectively, protect critical information infrastructures and safeguard data.***

Amendment 2

Proposal for a directive
Recital 1 a (new)

Text proposed by the Commission	*Amendment*
	(1a) Information systems are vital to political, social and economic interaction in the Union. Society is ever more dependent on information systems. However, despite their major benefits, they also embody a number of risks to our security because of their complexity and vulnerability to various types of cybercrime. The security of information systems is therefore a constant concern and requires effective responses from the Member States and from the Union.

Amendment 3

Proposal for a directive
Recital 2

Text proposed by the Commission	*Amendment*
(2) Attacks against information systems***, in particular as a result of the threat from organised crime,*** are a growing menace***, and*** there is increasing concern about the potential for terrorist or politically motivated attacks against information systems which form part of the critical infrastructure of Member States and the Union. This constitutes a threat to the achievement of a safer information society and an area of freedom, security and justice, and therefore requires a response at the level of the European Union.	(2) Attacks against information systems are a growing menace***. Theymay arise from terrorism or organised crime and they may be perpetrated by states or individuals.*** There is increasing concern about the potential for terrorist or politically motivated attacks against information systems which form part of the critical infrastructure of Member States and the Union. ***The cross-border nature of certain infringements and the relatively low risks and costs to perpetrators, coupled with the potentially high returns and resulting damage inflicted, seriously increases the risk of such attacks.*** This constitutes a threat to the achievement of a safer information society and an area of freedom, security and justice, and therefore requires a response ***not only*** at the level of the European Union ***but also the international community***.

Amendment 4

Proposal for a directive
Recital 3

Text proposed by the Commission	*Amendment*
(3) There is evidence of a tendency towards increasingly dangerous and recurrent large scale attacks conducted against information systems which are critical to ***states*** or to particular functions in the public or private sector. This tendency is accompanied by the development of increasingly sophisticated tools that can be used by criminals to launch cyber-attacks of various types.	(3) There is evidence of a tendency towards increasingly dangerous and recurrent large scale attacks conducted against information systems which are critical to ***Member States, to the Union*** or to particular functions in the public or private sector***, as well as at Union level***. This tendency is accompanied by the ***rapid*** development of ***computer technology and, as a result, increasingly*** sophisticated tools that can be used by criminals to launch cyber-attacks of various types, ***some of which have a great potential to cause economic and social damage***.

Amendment 5

Proposal for a directive
Recital 4 a (new)

Text proposed by the Commission	*Amendment*
	(4a) A thorough, reliable and independent assessment of the overall level of threat of attacks against information systems should be carried out. The Union institutions should adjust their level of information security accordingly.

Amendment 6

Proposal for a directive
Recital 4 b (new)

Text proposed by the Commission	*Amendment*
	(4b) There is a need for coordination at the level of the Union to help integrate different initiatives, programmes and activities.

Amendment 7

Proposal for a directive
Recital 6

Text proposed by the Commission	*Amendment*
(6) Member States should provide for penalties in respect of attacks against information systems. The penalties provided for should be effective, proportionate and dissuasive.	(6) Member States should provide for penalties in respect of attacks against information systems***, as part of a broader set of national strategies designed to deter and combat attacks of this nature.*** The penalties provided for should be effective, proportionate and dissuasive. ***Given the cross-border nature of the threats, it is necessary for Member States to align their penalties and thereby reduce the differences in their treatment of***

infringements across the Union.

Amendment 8

Proposal for a directive
Recital 8 a (new)

Text proposed by the Commission	*Amendment*
	(8a) The Council and the Commission should call on those Member States which still need to ratify the Council of Europe Convention on Cybercrime to do so without delay.

Amendment 9

Proposal for a directive
Recital 11 a (new)

Text proposed by the Commission	*Amendment*
	(11a) Cooperation on the part of the authorities with the private sector and civil society is of major importance in avoiding and combating cyber attacks. It is necessary to establish ongoing dialogue with them, given their extensive use of computer systems and the need for shared responsibility in ensuring reliable and functional systems. It is important to raise awareness among all computer system stakeholders, so as to create a data security mentality.

Amendment 10

Proposal for a directive
Recital 11b (new)

Text proposed by the Commission	*Amendment*
	(11b) Recent initiatives and projects relating to cyberdefence, such as within

	the European Defence Agency (EDA), should be encouraged to support the cyberdefence capabilities of Member States. Closer cooperation should be envisaged both with the EDA and with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), in particular in the field of capacity building and training.

Amendment 11

Proposal for a directive
Recital 12

Text proposed by the Commission	*Amendment*
(12) There is a need to collect data on offences under this Directive, in order to gain a more complete picture of the problem at Union level and thereby contribute to formulating more effective responses. The data will moreover help specialised agencies such as Europol and the European Network and Information Security Agency to better assess the extent of cybercrime and the state of network and information security in Europe.	(12) There is a need to collect data on offences under this Directive, in order to gain a more complete picture of the problem at Union level and thereby contribute to formulating more effective responses. ***Member States should step up exchanges of information regarding cyber attacks with the support of the Commission and the European Network and Information Security Agency.*** The data will moreover help specialised agencies such as Europol and the European Network and Information Security Agency to better assess the extent ***and impact*** of cybercrime and the state of network and information security in Europe. ***Improved knowledge of present and future risks will make it possible to take decisions which are more effective in deterring and combating cyber attacks or reducing the resulting damage.***

Amendment 12

Proposal for a directive
Recital 12 a (new)

Text proposed by the Commission	*Amendment*
	(12a) The Exchange of information and public-private partnerships (PPP) play an important role in improving cyber security. The Commission should therefore examine the feasibility of providing frameworks or instruments to help PPPs to cooperate with each other at national and Union level, in order to implement information quality standards for interoperability, and to ensure respect for fundamental rights, the separation of powers and democratic supervision.

Amendment 13

Proposal for a directive
Recital 13

Text proposed by the Commission	*Amendment*
(13) Significant gaps and differences in Member States' laws in the area of attacks against information systems area may hamper the fight against organised crime and terrorism, and may complicate effective police and judicial cooperation in this area. The transnational and borderless nature of modern information systems means that attacks against such systems have a trans-border dimension, thus underlining the urgent need for further action to approximate criminal legislation in this area. Besides that, the coordination of prosecution of cases of attacks against information systems should be facilitated by the adoption of Council Framework Decision 2009/948/JHA on prevention and settlement of conflict of jurisdiction in criminal proceedings.	(13) Significant gaps and differences in Member States' laws in the area of attacks against information systems area may hamper the fight against organised crime and terrorism, and may complicate effective police and judicial cooperation in this area. The transnational and borderless nature of modern information systems means that attacks against such systems have a trans-border dimension, thus underlining the urgent need for further action to approximate criminal legislation in this area ***at Union level. The Union should also seek greater international cooperation in the field of data network security by collaborating closely with other organisations with the relevant terms of reference, such as the United Nations, NATO, the Council of Europe, or the OSCE and involving other***

	international stakeholders. Besides that, the coordination of prosecution of cases of attacks against information systems should be facilitated by the adoption of Council Framework Decision 2009/948/JHA on prevention and settlement of conflict of jurisdiction in criminal proceedings.

Amendment 14

Proposal for a directive
Recital 16

Text proposed by the Commission	*Amendment*
(16) This Directive ***respects*** the fundamental rights and ***observes*** the principles recognised in particular by the Charter of Fundamental Rights of the European Union, including the protection of personal data, freedom of expression and information, the right to a fair trial, presumption of innocence and the rights of the defence, as well as the principles of legality and proportionality of criminal offences and penalties. In particular, this Directive seeks to ensure full respect for these rights and principles and must be implemented accordingly.	(16) This Directive ***and any practical application thereof respect*** the fundamental rights***, in particular the right to privacy,*** and ***observe*** the principles recognised in particular by the Charter of Fundamental Rights of the European Union, including the protection of personal data, freedom of expression and information, the right to a fair trial, presumption of innocence and the rights of the defence, as well as the principles of legality and proportionality of criminal offences and penalties. In particular, this Directive seeks to ensure full respect for these rights and principles and must be implemented accordingly. ***The free and open nature of the internet is not adversely affected by this Directive.***

Amendment 15

Proposal for a directive
Recital 16 a (new)

Text proposed by the Commission	*Amendment*
	(16a) The Council and the Commission should insist, in negotiations and in the course of their cooperation with third countries, on minimum requirements for preventing and fighting cybercrime and

cyber attacks as well as on minimum standards for information system security.

Amendment 16

Proposal for a directive
Recital 16 b (new)

Text proposed by the Commission	*Amendment*
	(16b) The Commission should consider options to facilitate and assist third countries in their efforts to develop their cyber security and cyber defence capabilities.

Amendment 17

Proposal for a directive
Article 14 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2a. The Commission shall assist Member States in promoting the resilience and stability of the internet and shall undertake other activities aiming at achieving information security.

Amendment 18

Proposal for a directive
Article 14 – paragraph 2 b (new)

Text proposed by the Commission	*Amendment*
	2b. The Council shall clarify the role of the Political and Security Committee and its other bodies in the context of dealing with potential cyberattacks.

Amendment 19

Proposal for a directive
Article 14 – paragraph 2 c (new)

Text proposed by the Commission	*Amendment*
	2c. Member States shall improve the exchange of information relating to cyber security. Members States, with the support of the Commission, should seek interactions with third countries, especially those from where the attacks most often originate.

Amendment 20

Proposal for a directive
Article 15 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall transmit the data collected according to this Article to the Commission. They shall also ensure that a consolidated review of these statistical reports is published.	3. Member States shall transmit the data collected according to this Article to the Commission. They shall also ensure that a consolidated review of these statistical reports is ***submitted to the European Parliament and*** published.

Amendment 21

Proposal for a directive
Article 15 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. A Union Cybersecurity Coordinator shall be appointed in order to facilitate the integration and coordination of Union initiatives, programmes and activities across Union institutions.

PROCEDURE

Title	Attacks against information systems and repealing Council Framework Decision 2005/222/JHA
References	COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)
Committee responsible Date announced in plenary	LIBE 7.10.2010
Committee(s) asked for opinion(s) Date announced in plenary	AFET 7.4.2011
Rapporteur(s) Date appointed	Kristiina Ojuland 29.3.2011
Date adopted	22.11.2011
Result of final vote	+: 38 –: 8 0: 0
Members present for the final vote	Sir Robert Atkins, Frieda Brepoels, Elmar Brok, Marietta Giannakou, Andrzej Grzyb, Takis Hadjigeorgiou, Anna Ibrisagic, Othmar Karas, Ioannis Kasoulides, Tunne Kelam, Evgeni Kirilov, Andrey Kovatchev, Eduard Kukan, Krzysztof Lisek, Sabine Lösing, Ulrike Lunacek, Barry Madlener, Francisco José Millán Mon, Annemie Neyts-Uyttebroeck, Raimon Obiols, Justas Vincas Paleckis, Ioan Mircea Paşcu, Cristian Dan Preda, Libor Rouček, José Ignacio Salafranca Sánchez-Neyra, Jacek Saryusz-Wolski, Werner Schulz, Marek Siwiec, Charles Tannock, Inese Vaidere, Kristian Vigenin, Sir Graham Watson
Substitute(s) present for the final vote	Laima Liucija Andrikienė, Elena Băsescu, Tanja Fajon, Diogo Feio, Monica Luisa Macovei, Emilio Menéndez del Valle, György Schöpflin, Traian Ungureanu, Ivo Vajgl, Renate Weber, Janusz Władysław Zemke
Substitute(s) under Rule 187(2) present for the final vote	Luís Paulo Alves, Sylvie Guillaume, Vladimir Urutchev

11.11.2011

OPINION OF THE COMMITTEE ON INDUSTRY, RESEARCH AND ENERGY

for the Committee on Civil Liberties, Justice and Home Affairs

on the proposal for a directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

Rapporteur: Christian Ehler

AMENDMENTS

The Committee on Industry, Research and Energy calls on the Committee on Civil Liberties, Justice and Home Affairs, as the committee responsible, to incorporate the following amendments in its report:

Amendment 1

Proposal for a directiveRecital 1

Text proposed by the Commission	*Amendment*
(1) The objective of this Directive is to approximate rules on criminal law in the Member States in the area of attacks against information systems, and improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States.	(1) ***Forming part of the Union's general strategy aimed at combating organised crime, increasing the resilience of computer networks, protecting critical information infrastructure and data protection,*** the objective of this Directive is to approximate rules on criminal law in the Member States in the area of attacks against information systems, and improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States***, the Commission, Eurojust, Europol, Union and national computer emergency response teams and the European***

	Network and Information Security Agency, to enable a common and comprehensive Union approach.

Amendment 2

Proposal for a directive
Recital 1 a (new)

Text proposed by the Commission	*Amendment*
	(1a) Information systems are a key element of political, social and economic interaction in Europe. Society is highly and increasingly dependent on such systems. The smooth operation and security of these systems in Europe is vital for the development of the internal market and of a competitive and innovative economy. At the same time as providing great benefits, however, information systems carry a number of risks to our security on account of their complexity and vulnerability to various types of computer crime. The security of information systems is thus a matter of constant concern that requires an effective response from the Member States and the Union.

Amendment 3

Proposal for a directive
Recital 2

Text proposed by the Commission	*Amendment*
(2) Attacks against information systems, ***in particular as a result of the threat*** from organised crime, are a growing menace, and there is increasing concern about the potential for terrorist or politically motivated attacks against information systems which form part of the critical infrastructure of Member States and the Union. This constitutes a threat to the	(2) Attacks against information systems ***may come*** from ***a variety of actors such as terrorists,*** organised crime ***groups, countries or isolated individuals. They*** are a growing menace ***to the functioning of information systems in the Union and globally***, and there is increasing concern about the potential for terrorist or politically motivated attacks against

achievement of a safer information society and an area of freedom, security and justice, and therefore requires a response at the level of the European Union.	information systems which form part of the critical infrastructure of Member States and the Union. ***The cross-border nature of certain offences and the relatively low risk and cost for offenders, coupled with the huge benefits that may be gained and damage that may be caused through the attacks, adds greatly to the level of this menace.*** This constitutes a threat to the achievement of a safer information society and an area of freedom, ***democracy,*** security and justice, ***undermines the creation of a European digital internal market*** and therefore requires a response at the level of the European Union ***as well as internationally, for example through the 2001 Council of Europe Convention on Cybercrime***.

Amendment 4

Proposal for a directive
Recital 2 a (new)

Text proposed by the Commission	*Amendment*
	(2a) Recent cyber attacks perpetrated against European networks or information systems have caused substantial economic and security damage to the Union.

Justification

Having regard to the March 2011 cyber-attacks on the European institutions, as well as to the numerous breaches in the European Emissions Trading Systems, which all resulted by thefts of millions of EUR in emissions;

Amendment 5

Proposal for a directive
Recital 3

Text proposed by the Commission	*Amendment*
(3) There is evidence of a tendency	(3) There is evidence of a tendency

towards increasingly dangerous and recurrent large scale attacks conducted against information systems which are critical to *states* or to particular functions in the public or private sector. This tendency is accompanied by the development of increasingly sophisticated tools that can be used by criminals to launch cyber-attacks of various types.	towards increasingly dangerous and recurrent large scale attacks***, including distributed denial-of-service attacks,*** conducted against information systems which are critical to ***international organisations,*** *countries****, the Union*** or to particular functions in the public or private sector. ***Such attacks can cause substantial economic damage both through interruption of information systems and communications themselves and through loss or alteration of commercially important confidential information or other data. Innovative SMEs, dependent on the proper functioning and availability of information systems while potentially able to devote fewer resources to information security, risk being especially affected.*** This tendency is accompanied by the ***rapid*** development of ***information technology and thus of*** increasingly sophisticated tools that can be used by criminals to launch cyber-attacks of various types***, some of which have significant potential to cause economic and social damage***.

Amendment 6

Proposal for a directive
Recital 4

Text proposed by the Commission	*Amendment*
(4) Common definitions in this area, particularly of information systems ***and*** computer data, are ***important*** in order to ensure a consistent approach in the Member States to the application of this Directive.	(4) Common definitions in this area, particularly of information systems***,*** computer data ***and criminal offences in respect of information systems and computer data*** are ***essential*** in order to ensure a consistent ***and uniform*** approach in the Member States to the application of this Directive.

Amendment 7

Proposal for a directive
Recital 6

Text proposed by the Commission	*Amendment*
(6) Member States should provide for penalties in respect of attacks against information systems. The penalties provided for should be effective, proportionate and dissuasive.	(6) ***In addition to measures by Member States, the Union and the private sector aimed at increasing the security and integrity of information systems and at preventing attacks and minimising their impact,*** Member States should provide ***both*** for ***effective measures to prevent such attacks and for harmonised*** penalties in respect of attacks against information systems***, which should be adopted within broader national strategies to deter and combat such attacks***. The penalties provided for should be effective, proportionate and dissuasive. ***Convergence in the sanctions and penalties applied by Member States is necessary on account of the often cross-border nature of the threats and is aimed at reducing differences between Member States when it comes to dealing with offences committed within the Union.***

Amendment 8

Proposal for a directive
Recital 6 a (new)

Text proposed by the Commission	*Amendment*
	(6a) Member States, the Union and the private sector, in cooperation with the European Network and Information Security Agency, should take steps to increase the security and integrity of information systems, to prevent attacks and to minimise the impact of attacks.

Amendment 9

Proposal for a directive
Recital 8

Text proposed by the Commission	*Amendment*
(8) The Council Conclusions of 27-28 November 2008 indicated that a new strategy should be developed with the Member States and the Commission, taking into account the content of the 2001 Council of Europe Convention on Cybercrime. That Convention is the legal framework of reference for combating cybercrime, including attacks against information systems. This Directive ***builds on*** that Convention.	(8) The Council Conclusions of 27-28 November 2008 indicated that a new strategy should be developed with the Member States and the Commission, taking into account the content of the 2001 Council of Europe Convention on Cybercrime. ***The Council and the Commission should encourage Member States that have not yet ratified the Convention to do so as soon as possible.*** That Convention is the legal framework of reference for combating cybercrime, including attacks against information systems. This Directive ***takes into account the relevant provisions of*** that Convention.

Amendment 10

Proposal for a directive
Recital 10

Text proposed by the Commission	*Amendment*
(10) This Directive does not intend to impose criminal liability where the ***offences are*** committed without criminal intent, such as for authorised testing or protection of information systems.	(10) This Directive does ***not cover action taken to ensure the security of information systems, such as the ability of an information system to resist criminal acts as defined in this Directive, or to have tools used or intended to be used for such actions removed from them. It also does*** not intend to impose criminal liability where the ***objective criteria of the crimes listed in this Directive are met but the action is*** committed without criminal intent, such as for authorised testing or protection of information systems.

Justification

Given the sometimes blurry boundary between malicious and non-malicious access

(automatic updates etc) the amendment aims at making clear that e.g. the operation of anti-virus software or virus removal tools, or the quarantining of infected devices, are entirely outside the scope of the Directive.

Amendment 11

Proposal for a directive
Recital 11

Text proposed by the Commission	*Amendment*
(11) This Directive strengthens the importance of networks, such as the G8 or the Council of Europe's network of points of contact available on a twenty-four hour, seven-day-a-week basis to exchange information in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to information systems and data, or for the collection of evidence ***in electronic form*** of a criminal offence. Given the speed with which large-scale attacks can be carried out, Member States should be able to respond promptly to urgent requests from this network of contact points. Such assistance should include facilitating, or directly carrying out, measures such as: the provision of technical ***advice***, the preservation of data, the collection of evidence, the provision of legal information, and the locating of suspects.	(11) This Directive strengthens the importance of networks, such as the G8 or the Council of Europe's network of points of contact available on a twenty-four hour, seven-day-a-week basis to exchange information in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to information systems and data, or for the collection of evidence of a criminal offence ***or intent to commit a criminal offence***. Given the speed with which large-scale attacks can be carried out, Member States ***the Union and the European Network and Information Security Agency*** should be able to respond promptly ***and effectively*** to urgent requests from this network of contact points. Such assistance should include facilitating, or directly carrying out, measures such as: the provision of technical assistance, ***including as regards restoring information system functionality,*** the preservation of data ***in line with personal data protection principles***, the collection of evidence, the provision of legal information, ***the identification of the jeopardised and/or extracted information*** and the locating ***and identification*** of suspects.

Amendment 12

Proposal for a directive
Recital 11 a (new)

Text proposed by the Commission	*Amendment*
	(11a) Cooperation by the public authorities with the private sector and civil society is of great importance in preventing and combating attacks against information systems. A permanent dialogue should be established with these partners in view of the extensive use they make of information systems and the sharing of responsibility required for the stable and proper operation of these systems. The raising of awareness among all stakeholders in the use of information systems is important in creating a culture of IT security.

Amendment 13

Proposal for a directive
Recital 12

Text proposed by the Commission	*Amendment*
(12) There is a need to collect data on offences under this Directive, in order to gain a more complete picture of the problem at Union level and thereby contribute to formulating more effective responses. The data will moreover help specialised agencies such as Europol and the European Network and Information Security Agency to better assess the extent of cybercrime and the state of network and information security in Europe.	(12) There is a need to collect data on offences under this Directive, in order to gain a more complete picture of the problem at Union level and thereby contribute to formulating more effective responses. ***Member States need to improve the exchange of information on attacks against information systems, with the support of the Commission and the European Network and Information Security Agency.*** The data will moreover help specialised ***bodies and*** agencies such as ***Member States' CERTs,*** agencies such as Europol and the European Network and Information Security Agency to better assess the extent of cybercrime and the state of network and information security in ***the Union and to support Member States in the adoption of responses to information security incidents***. ***Better knowledge about present and future risks will help reach more appropriate***

decisions on deterring, combating or limiting the damage caused by attacks against information systems.

Amendment 14

Proposal for a directive
Recital 12 a (new)

Text proposed by the Commission	*Amendment*
	(12a) While this Directive must meet stringent requirements for legal certainty and foreseeability in criminal law, there is also a need, met through the provisions of this Directive on collection of data, exchange of information and the obligation on the Commission to report regularly on its application and to make any necessary proposals, to provide for a flexible mechanism to enable adaptation to future developments, possibly leading to a broadening of the scope of this Directive. Such future developments include any technological developments enabling for example more effective enforcement in the area of attacks against information systems or which facilitate prevention or mitigation of such attacks.

Justification

While the introduction of penalties is appreciated a comprehensive Union approach to tackle cybercrime should not only focus on effective law enforcement but also develop strategies and instruments to prevent those criminal activities.

Amendment 15

Proposal for a directive
Recital 12 b (new)

Text proposed by the Commission	*Amendment*
	(12b) The European Network and Information Security Agency should play a strategic role in coordination the efforts

	of Member States and the Union institutions. The Agency may, for example, be tasked with supervising the exchange of information between them, thus functioning as a single point of contact and as the Union's cybersecurity incident registrar. It may also be tasked with centralising statistical data on offences referred to in this Directive at Union level and to use it as a basis for drawing up reports on the state of information systems and computer data security across the Union.

Amendment 16

Proposal for a directive
Recital 13

Text proposed by the Commission	*Amendment*
(13) Significant gaps and differences in Member States' laws in the area of attacks against information systems area may hamper the fight against organised crime and terrorism, and may complicate effective police and judicial cooperation in this area. The transnational and borderless nature of modern information systems means that attacks against such systems have a trans-border dimension, thus underlining the urgent need for further action to approximate criminal legislation in this area. Besides that, the coordination of prosecution of cases of attacks against information systems should be facilitated by the adoption of Council Framework Decision 2009/948/JHA on prevention and settlement of conflict of jurisdiction in criminal proceedings.	(13) Significant gaps and differences in Member States' laws in the area of attacks against information systems area may hamper the fight against organised crime and terrorism, and may complicate effective police and judicial cooperation in this area. The transnational and borderless nature of modern information systems means that attacks against such systems have a trans-border dimension, thus underlining the urgent need for further action ***at Union level*** to approximate ***national*** criminal legislation in this area. ***Likewise, the Union should pursue greater international cooperation in the field of network and information system security involving all relevant international actors.*** Besides that, the coordination of prosecution of cases of attacks against information systems should be facilitated by the adoption of Council Framework Decision 2009/948/JHA on prevention and settlement of conflict of jurisdiction in criminal proceedings.

Amendment 17

Proposal for a directive
Article 1 – paragraph 1

Text proposed by the Commission	*Amendment*
This Directive defines criminal offences in the area of attacks against information systems and establishes minimum rules concerning penalties for such offences. It also aims to introduce common provisions to prevent such attacks and improve European ***criminal justice*** cooperation in this field.	This Directive defines criminal offences in the area of attacks against information systems and establishes ***harmonised*** minimum rules concerning penalties for such offences. It also aims to introduce common provisions ***both*** to prevent ***and combat*** such attacks and ***to*** improve European cooperation in this field***, particularly as regards criminal justice***.

Amendment 18

Proposal for a directive
Article 2 – point d

Text proposed by the Commission	*Amendment*
(d) "without right" means access or interference not authorised by the owner, other right holder of the system or of part of it, or not permitted under national ***legislation***.	(d) "without right" means access or interference not authorised by the owner, other right holder of the system or of part of it, or not permitted under national ***or Union law***.

Amendment 19

Proposal for a directive
Article 7 – point b

Text proposed by the Commission	*Amendment*
(b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.	(b) a computer password, access code, ***a digital*** or ***physical security token, or*** similar data by which the whole or any part of an information system is capable of being accessed.

Amendment 20

Proposal for a directive
Article 8 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	1a. Member States shall ensure that the unauthorised forwarding of identification data to other persons with a view to the conduct of any of the activities referred to in Articles 3 to 7 is a criminal offence.

Amendment 21

Proposal for a directive
Article 8 – paragraph 1 b (new)

Text proposed by the Commission	*Amendment*
	1b. Member States shall ensure that an offence under Articles 3 to 7 committed by a person who, within the scope of his or her employment, has access to the security systems inherent in information systems, is treated as an aggravating circumstance and is a criminal offence.

Amendment 22

Proposal for a directive
Article 10 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 6 are punishable by criminal penalties of a maximum term of imprisonment of at least five years when committed through the use of a tool designed to launch attacks affecting a significant number of information systems, or attacks causing considerable damage, such as disrupted system services, financial cost or loss of personal data.	2. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 6 are punishable by criminal penalties of a maximum term of imprisonment of at least five years when committed through the use of a tool designed to launch attacks affecting a significant number of information systems, or attacks causing considerable damage, such as disrupted system services, financial cost or loss of personal data ***or sensitive information***.

Amendment 23

Proposal for a directive
Article 13 – paragraph 1 – point c

Text proposed by the Commission	*Amendment*
(c) for the benefit of a legal person ***that has its head office*** in the territory of the Member State concerned.	(c) for the benefit of a legal person ***incorporated*** in the territory of the Member State concerned.

Amendment 24

Proposal for a directive
Article 14 – paragraph 1

Text proposed by the Commission	*Amendment*
1. For the purpose of exchange of information relating to the offences referred to in Articles 3 to 8, and in accordance with data protection rules, Member States shall make use of the ***existing*** network of operational points of contact available 24 hours a day and seven days a week. Member States shall also ensure that they have procedures in place so that they can respond within a maximum of eight hours to urgent requests. Such response shall ***at least*** indicate ***whether and in what*** form ***the request for help will be answered and when***.	1. For the purpose of exchange of information relating to the offences referred to in Articles 3 to 8, and in accordance with data protection rules, Member States shall ***ensure that they have an operational national point of contact and*** make use of the network of operational points of contact available 24 hours a day and seven days a week ***and also forward such information to the Commission and the European Network and Information Security Agency***. Member States shall also ensure that they have procedures in place so that they can respond within a maximum of eight hours to urgent requests. Such response ***shall be effective and shall include, where appropriate, the facilitation or direct implementation of the following measures: the provision of technical advice, including as regards restoring information system functionality, the preservation of data in line with personal data protection principles***, ***the collection of evidence, the provision of legal information, and the locating and identification of suspects. The points of contact*** shall indicate ***the***

form ***and timescale in which requests for assistance will be answered***.

Amendment 25

Proposal for a directive
Article 14 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall inform the Commission of their appointed point of contact for the purpose of exchanging information on the offences referred to in Articles 3 to 8. The Commission shall forward that information to the other Member States.	2. Member States shall inform the Commission***, Eurojust and the European Network and Information Security Agency*** of their appointed point of contact for the purpose of exchanging information on the offences referred to in Articles 3 to 8. The Commission shall forward that information to the other Member States.

Amendment 26

Proposal for a directive
Article 15 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall transmit the data collected according to this Article to the Commission. ***They*** shall also ensure that a consolidated review of these statistical reports is published.	3. Member States shall transmit the data collected according to this Article to the Commission***, Europol and the European Network and Information Security Agency and*** shall also ensure that a consolidated ***periodic*** review of these statistical reports is published.

Amendment 27

Proposal for a directive
Article 18 – paragraph 1

Text proposed by the Commission	*Amendment*
1. By [FOUR YEARS FROM ADOPTION] and every three years thereafter, the Commission shall submit a	1. By [FOUR YEARS FROM ADOPTION] and every three years thereafter, the Commission shall***, after***

report to the European Parliament and the Council on the application of this Directive in the Member States including any necessary proposal.	***having consulted all relevant stakeholders,*** submit a report to the European Parliament and the Council on the application of this Directive in the Member States including any necessary proposal***. Each report shall identify, and take into account with respect to any necessary proposal, technical solutions enabling a more effective enforcement in the Union in the area of attacks against information systems, including technical solutions which could serve to prevent or mitigate such attacks.***

Amendment 28

Proposal for a directive
Article 18 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall send to the Commission all the information that is appropriate for drawing up the report referred to in paragraph 1. The information shall include a detailed description of legislative and non-legislative measures adopted in implementing this Directive.	2. Member States ***and the European Network and Information Security Agency*** shall send to the Commission all the information that is appropriate for drawing up the report referred to in paragraph 1. The information shall include a detailed description of legislative and non-legislative measures adopted in implementing this Directive.

PROCEDURE

Title	Attacks against information systems and repealing Council Framework Decision 2005/222/JHA
References	COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)
Committee responsible Date announced in plenary	LIBE 7.10.2010
Committee(s) asked for opinion(s) Date announced in plenary	ITRE 7.10.2010
Rapporteur(s) Date appointed	Christian Ehler 24.11.2010
Discussed in committee	13.4.2011 6.10.2011
Date adopted	10.11.2011
Result of final vote	+: 49 –: 0 0: 1
Members present for the final vote	Ivo Belet, Bendt Bendtsen, Maria Da Graça Carvalho, Giles Chichester, Pilar del Castillo Vera, Christian Ehler, Ioan Enciu, Adam Gierek, Norbert Glante, Robert Goebbels, Fiona Hall, Jacky Hénin, Kent Johansson, Romana Jordan Cizelj, Lena Kolarska-Bobińska, Béla Kovács, Philippe Lamberts, Bogdan Kazimierz Marcinkiewicz, Marisa Matias, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Aldo Patriciello, Anni Podimata, Miloslav Ransdorf, Herbert Reul, Michèle Rivasi, Jens Rohde, Paul Rübig, Amalia Sartori, Francisco Sosa Wagner, Konrad Szymański, Michael Theurer, Ioannis A. Tsoukalas, Claude Turmes, Niki Tzavela, Marita Ulvskog, Vladimir Urutchev, Adina-Ioana Vălean
Substitute(s) present for the final vote	Antonio Cancian, Jolanta Emilia Hibner, Yannick Jadot, Ivailo Kalfin, Bernd Lange, Werner Langen, Markus Pieper, Mario Pirillo, Hannes Swoboda, Silvia-Adriana Ţicău
Substitute(s) under Rule 187(2) present for the final vote	Eider Gardiazábal Rubial

PROCEDURE

Title	Attacks against information systems and repealing Council Framework Decision 2005/222/JHA			
References	COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)			
Date submitted to Parliament	30.9.2010			
Committee responsible Date announced in plenary	LIBE 7.10.2010			
Committee(s) asked for opinion(s) Date announced in plenary	AFET 7.4.2011	BUDG 7.10.2010	ITRE 7.10.2010	
Not delivering opinions Date of decision	BUDG 20.10.2010			
Rapporteur(s) Date appointed	Monika Hohlmeier 9.12.2010			
Discussed in committee	3.2.2011	25.5.2011	12.1.2012	28.2.2012
	27.3.2012	21.6.2012	6.6.2013	
Date adopted	6.6.2013			
Result of final vote	+: –: 0:	36 8 0		
Members present for the final vote	Jan Philipp Albrecht, Emine Bozkurt, Arkadiusz Tomasz Bratkowski, Philip Claeys, Carlos Coelho, Ioan Enciu, Frank Engel, Cornelia Ernst, Kinga Gál, Kinga Göncz, Sylvie Guillaume, Sophia in 't Veld, Lívia Járóka, Teresa Jiménez-Becerril Barrio, Juan Fernando López Aguilar, Baroness Sarah Ludford, Monica Luisa Macovei, Svetoslav Hristov Malinov, Véronique Mathieu Houillon, Nuno Melo, Roberta Metsola, Antigoni Papadopoulou, Georgios Papanikolaou, Jacek Protasiewicz, Carmen Romero López, Birgit Sippel, Csaba Sógor, Rui Tavares, Nils Torvalds, Wim van de Camp, Axel Voss, Josef Weidenholzer, Cecilia Wikström, Tatjana Ždanoka, Auke Zijlstra			
Substitute(s) present for the final vote	Dimitrios Droutsas, Mariya Gabriel, Evelyne Gebhardt, Stanimir Ilchev, Franziska Keller, Jean Lambert, Jan Mulder			
Substitute(s) under Rule 187(2) present for the final vote	Jens Nilsson, Sabine Verheyen			
Date tabled	19.6.2013			