EUROPEAN PARLIAMENT 2009 - 2014

Committee on Industry, Research and Energy

2010/0273(COD)

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

PA_Legam

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 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) ***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 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 ***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 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 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***, 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	(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.

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	2. Member States shall inform the Commission***, Eurojust and the European***

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.	***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 report to the European Parliament and the Council on the application of this Directive in the Member States including any necessary proposal.	1. By [FOUR YEARS FROM ADOPTION] and every three years thereafter, the Commission shall***, after 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