EUROPEAN PARLIAMENT 2009 - 2014

Committee on Industry, Research and Energy

2010/0273(COD)

12.10.2011

AMENDMENTS
12 - 55

Draft opinion
Christian Ehler
(PE472.192v01-00)

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

Proposal for a directive
(COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

AM_Com_LegOpinion

Amendment 12
Teresa Riera Madurell

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 the Union; this objective forms 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.***

Or. es

Amendment 13
Ioan Enciu

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***,*** other specialised law enforcement services of the Member States***, and the Commission, Eurojust, Europol and the European Network and Information Security Agency, to enable a common and comprehensive Union approach***.

Or. ro

Amendment 14
Ioannis A. Tsoukalas

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***, the Commission, ENISA, EUROPOL and EUROJUST to enable a common and comprehensive Union approach***.

Or. en

Amendment 15
Ivailo Kalfin

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***, ENISA, national Computer Emergency Response Teams (CERTs),*** and other specialised law enforcement services of the Member States.

Or. en

Amendment 16
Teresa Riera Madurell

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 European single 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.

Or. es

Amendment 17
Teresa Riera Madurell

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	(2) Attacks against information systems are a growing menace and ***may come from a variety of actors such as terrorists, organized crime, States or isolated individuals. There*** is increasing concern about the potential for terrorist or politically motivated attacks against

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.

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, security and justice, and therefore requires a response ***not just*** at the level of the European Union ***but also by the international community***.

Or. es

Amendment 18
Ioannis A. Tsoukalas

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, in particular as a result of the threat from organised crime, 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. 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 single 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***.

Or. en

Amendment 19
Ioan Enciu

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, in particular as a result of the threat from organised crime, are a growing menace ***both 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. 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 coordination and cooperation at international level***.

Or. ro

Amendment 20
Ivailo Kalfin

Proposal for a directive
Recital 2 a (new)

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

Or. en

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 21
Silvia-Adriana Ţicău

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 ***international organisations and*** states or to particular functions in the public or private sector. ***Such attacks can occasion significant financial losses both by taking down information and communications systems, and by causing the loss or alteration of data.*** This tendency is ***being*** accompanied***, unfortunately,*** by the ***availability and*** development of increasingly sophisticated tools that can be used by criminals to launch cyber-attacks of various types.

Or. ro

Amendment 22
Ivailo Kalfin

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	(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.

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. ***Furthermore, distributed denial-of-service attacks on information systems and/ or attacks on critical information infrastructures for disruption purposes might be used as a means of cyber warfare and/ or terrorism.***

Or. en

Amendment 23
Teresa Riera Madurell

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 states***, the Union*** or to particular functions in the public or private sector. 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***.

Or. es

Amendment 24
Ioan Enciu

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.

Or. ro

Amendment 25
Ivailo Kalfin

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 ***and norms of behaviour*** 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.

Or. en

Amendment 26
Francisco Sosa Wagner

Proposal for a directive
Recital 4 a (new)

Text proposed by the Commission	*Amendment*
	(4a) The revocation of IP addresses or domain names are examples of system interference and may be considered as criminal offences as defined in Article 4 of this Directive.

Or. en

Justification

The ITRE Report internet governance: the next steps states that governments should "protect the integrity of the global internet and freedom of communication by avoiding any regional measures, such as revocation of IP addresses or domain names in third countries". Revocation of IP addresses or domain names without right, e.g. without a prior court order, can seriously damage legal businesses, as well as impacting on freedom of communication. The recital clarifies that illegal system interference covers such actions in relation to the EU.

Amendment 27
Philippe Lamberts
on behalf of the Verts/ALE Group

Proposal for a directive
Recital 4 a (new)

Text proposed by the Commission	*Amendment*
	(4a) The revocation of IP addresses or domain names are examples of system interference and may be considered as criminal offences as defined in Article 4 of this Directive.

Or. en

Amendment 28
Teresa Riera Madurell

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 ***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.

Or. es

Amendment 29
Ioan Enciu

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 ***both*** for ***harmonised*** penalties in respect of attacks against information systems ***and for effective measures to prevent such attacks***. The penalties provided for should be effective, proportionate and dissuasive.

Or. ro

Amendment 30
Silvia-Adriana Ţicău

Proposal for a directive
Recital 6 a (new)

Text proposed by the Commission	*Amendment*
	(6a) Member States, the EU 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.

Or. ro

Amendment 31
Silvia-Adriana Ţicău

Proposal for a directive
Recital 7

Text proposed by the Commission	*Amendment*
(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, when the attack is conducted on a large scale, or when an offence is committed by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner. It is also appropriate to provide for more severe penalties where such an attack ***has caused*** serious damage or ***has affected*** essential interests.	(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, when the attack is conducted on a large scale, or when an offence is committed by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner. It is also appropriate to provide for more severe penalties where such an attack ***is carried out from within an organisation by someone with access rights and causes*** serious damage or ***affects*** essential interests.

Or. ro

Amendment 32
Teresa Riera Madurell

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	(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***

framework of reference for combating cybercrime, including attacks against information systems. This Directive builds on that Convention.

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 builds on that Convention.

Or. es

Amendment 33
Ioan Enciu

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 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, and the locating ***and identification*** of suspects.

Or. ro

Amendment 34
Silvia-Adriana Ţicău

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 in electronic form of a criminal offence. Given the speed with which large-scale attacks can be carried out, Member States ***the EU and the European Network and Information Security Agency*** 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.

Or. ro

Amendment 35
Ivailo Kalfin

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 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, ***the identification of the jeopardised and/or extracted information*** and the locating of suspects.

Or. en

Amendment 36
Teresa Riera Madurell

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.

Or. es

Amendment 37
Teresa Riera Madurell

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 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. ***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.***

Or. es

Amendment 38
Silvia-Adriana Ţicău

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. 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 ***and to support Member States in the adoption of responses to information security incidents***.

Or. ro

Amendment 39
Ivailo Kalfin

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. The data will moreover help specialised ***bodies and*** agencies such as ***Member States' CERTs,*** 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.

Or. en

Amendment 40
Teresa Riera Madurell

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.

Or. es

Amendment 41
Ioan Enciu

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	This Directive defines criminal offences in the area of attacks against information systems and establishes ***harmonised***

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.	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***.

Or. ro

Amendment 42
Ioan Enciu

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 European*** legislation.

Or. ro

Amendment 43
Ioannis A. Tsoukalas

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.

Or. en

Amendment 44
Silvia-Adriana Ţicău

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 punishable as a criminal offence.

Or. ro

Amendment 45
Silvia-Adriana Ţicău

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

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

Or. ro

Amendment 46
Ivailo Kalfin

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***.

Or. en

Amendment 47
Ioan Enciu

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. 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 ***must be effective and 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***.

Or. ro

Amendment 48
Ioannis A. Tsoukalas

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 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. ***ENISA may undertake this role and supervise the exchange of information, functioning as a single point of contact and as the Union's cybersecurity incident registrar.***

Or. en

Amendment 49
Silvia-Adriana Ţicău

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 ***forward such information to the Commission, the European Network and Information Security Agency and the other Member States, making*** 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.

Or. ro

Amendment 50
Ioan Enciu

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.

Or. ro

Amendment 51
Niki Tzavela

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

Text proposed by the Commission	*Amendment*
	2a. ENISA shall play a strategic role in the coordination efforts between Member States and the Union institutions.

Or. en

Amendment 52
Ioannis A. Tsoukalas

Proposal for a directive
Article 15 – paragraph 1

Text proposed by the Commission	*Amendment*
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 8.	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 8. ***In the case of offences involving more than one Member State, ENISA may facilitate the exchange of those data among all interested parties, including EUROPOL and EUROJUST.***

Or. en

Amendment 53
Ioan Enciu

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	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.	Commission ***and the European Network and Information Security Agency and*** shall also ensure that a ***periodic*** consolidated review of these statistical reports is published. ***The European Network and Information Security Agency shall centralise that data at an EU level and use it as a basis for drawing up reports on the state of information system and computer data security across Europe.***

Or. ro

Amendment 54
Silvia-Adriana Ţicău

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 ***and the European Network and Information Security Agency (ENISA)***. They shall also ensure that a consolidated review of these statistical reports is published.

Or. ro

Amendment 55
Ioan Enciu

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	2. Member States ***and the European Network and Information Security Agency*** shall send to the Commission all the information that is appropriate for

shall include a detailed description of legislative and non-legislative measures adopted in implementing this Directive.	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.

Or. ro